Oprogramowanie dla bankowości.

Dokumentacja użytkownika systemu Asseco EBP

aplikacja mobilna klienta

Version 4.5.0

asseco

Spis treści

1. **Konwencje typograficzne** . . . 2
2. **Słownik pojęć** . . . 4
3. **Wprowadzenie** . . . 5
4. **Aktywacja aplikacji** . . . 7
    4.1. Wprowadzenie kodu aktywacyjnego . . . 10
    4.2. Wprowadzenie kodu SMS . . . 15
    4.3. Wprowadzenie kodu PIN . . . 17
    4.4. Ustawienie metody logowania . . . 24
5. **Logowanie** . . . 30
    5.1. Logowanie - Ekran powitalny . . . 30
    5.2. Logowanie - Metoda autentykacji . . . 33
        5.2.1. Logowanie przy użyciu 'kodu PIN' . . . 34
        5.2.2. Logowanie przy użyciu metody biometrycznej . . . 37
        5.2.3. Prezentacja pulpitu po zalogowaniu . . . 41
6. **Autoryzacja dyspozycji** . . . 48
    6.1. Autoryzacja dyspozycji składanej ***wewnątrz*** aplikacji hybrydowej . . . 48
    6.2. Autoryzacja dyspozycji **zewnętrznej** przychodzącej ***przed zalogowaniem*** . . . 52
    6.3. Autoryzacja dyspozycji **zewnętrznej** przychodzącej ***po zalogowaniu*** . . . 61
7. **Rejestr autoryzacji** . . . 62
8. **Powiadomienia** . . . 66
    8.1. Powiadomienia PUSH . . . 66
    8.2. Lista powiadomień . . . 67
9. **Ustawienia** . . . 72
    9.1. Zarządzanie skrótami . . . 73
    9.2. Dane osobowe . . . 79
    9.3. Zmiana PIN . . . 80
    9.4. Dane biometryczne . . . 90
    9.5. Dezaktywacja aplikacji . . . 93
    9.6. Informacje o aplikacji . . . 98
10. **Wylogowanie** . . . 99

Informacje o dokumencie

Niniejszy dokument jest dokumentacją Użytkownika systemu Asseco Aplikacja hybrydowa w wersji {revnumber2}.

Metryka dokumentu:

Autor: Dział Systemów Omnikanałowych/ Pion Banków Komercyjnych
Wersja systemu: {revnumber2}
Wersja dokumentu: 1.00
Data wydania dokumentu: 2020-04-20
Przeznaczenie dokumentu: poufny, zewnętrzny
Identyfikator dokumentu: DOC.INST_Asseco_4.5.0

Historia zmian:

Data	Autor	Wersja systemu	Opis zmiany
2020-04-20	Agata Staszak	4.08.002C	Utworzenie dokumentacji
2020-08-11	Ewa Kumorek	4.08.002C	Aktualizacja dokumentacji
2020-09-15	Agata Staszak	4.13.000C	Aktualizacja dokumentacji

1. 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. *Dane archiwalne* → *Przeglądanie*.
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 przeksięgowań nie są kontrolowane przez system i wykonywane są wyłącznie na własną odpowiedzialność operatora!
Link	Odwołania do innych rozdziałów lub fragmentów tekstu. Adresy URL
Kod źródłowy	Fragmenty kodu źródłowego. Przykłady wydruków `{ "a": "b" }`

Konwencja typograficzna lub znak wizualny	Opis
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]

2. Słownik pojęć

Pojęcie	Opis
Aplikacja mobilna	Hybrydowa aplikacja mobilna działająca na urządzeniach przenośnych, takich jak smartfony czy tablety, powiązana z systemem Asseco CBP/EBP
Asseco CBP/EBP	System bankowości internetowej do obsługi klientów detalicznych i korporacyjnych dostarczany przez Asseco Poland S.A.
Użytkownik	Osoba fizyczna będąca reprezentantem klienta, której przydzielono dostęp internetowy do usług świadczonych przez Bank dla Klienta w systemie Asseco CBP/EBP. Posługuje się identyfikatorem użytkownika. Dysponuje urządzeniem z przeglądarką WWW i dostępem do Internetu lub urządzeniem mobilnym.
Asseco MAA	Aplikacja mobilna służąca do autoryzacji dyspozycji oraz logowania.
Metody biometryczne	Rodzaj zabezpieczenia oparty na danych biometrycznych użytkownika takich jak: wizerunek twarzy (Face ID) czy zapis linii papilarnych palców (odcisk palca)

3. Wprowadzenie

Aplikacja **hybrydowa** jest połączeniem funkcjonalności bankowości internetowej Asseco CBP/EBP oraz funkcjonalności autoryzacji i autentykacji poprzez urządzenia mobilne Asseco MAA.

Użytkownik posiadający dostęp do **Aplikacji hybrydowej** ma możliwość:

- autentykacji do aplikacji hybrydowej,
- autoryzacji logowania do systemu CBP/EBP,
- autoryzacji dyspozycji zleconych w systemie CBP/EBP,
- korzystania z podstawowych funkcjonalności zawartych w systemie CBP/EBP,
- zarządzania aplikacją hybrydową,
- obsługi powiadomiń PUSH.

Aplikacja zapewnia podstawowe funkcjonalności bankowości internetowej takie jak:

- Rachunki,
- Przelewy,
- Karty,
- Lokaty,
- Kredyty,
- Doładownia,
- Wnioski,
- Przepływy,
- Terminarz,
- Autodealing,
- Koszyk zleceń,
- Wiadomości,
- Ustawienia.

Aplikacja dostosowana jest do pracy zarówno na smartfonach jak i tabletach, dla urządzeń pracujących pod kontrolą systemu iOS oraz Android w wersjach:

iOS: dla wersji 9.0 i wyższej,

Android: dla wersji 6.0 i wyższej.

Aplikacja udostępniona jest w sklepach Google Play oraz App Store.

Dostęp do hybrydowej aplikacji mobilnej zabezpieczony jest jedną z metod wybraną przez użytkownika:

- kod PIN,
- metoda biometryczna

Dla logowania do aplikacji użyte zostały natywne sprzętowe funkcje urządzeń mobilnych, co oznacza, że logowanie z użyciem metod biometrycznych użytkownika dostępna jest tylko na urządzeniach posiadających takie funkcjonalności.

Autoryzacja dyspozycji w aplikacji realizowana jest poprzez moduł Asseco MAA, który stanowi integralną część hybrydowej aplikacji mobilnej.

Po zainstalowaniu aplikacji użytkownik w pierwszej kolejności musi powiązać aplikację z systemem Asseco CBP/EBP. Po poprawnym zakończeniu procesu powiązania hybrydowa aplikacja mobilna zostaje powiązana z kontem użytkownika i prezentowana na liście powiązanych aplikacji. Od tego momentu dostęp do pełnej funkcjonalności hybrydowej aplikacji mobilnej zabezpieczony jest wybraną przez użytkownika metodą: kod PIN lub metodą biometryczną. Prośba o jej użycie pojawia się bezpośrednio po uruchomieniu aplikacji.

W przypadku wyboru zabezpieczenia aplikacji mobilnej kodem PIN, kod ten służy również do autoryzacji zleceń wprowadzanych w hybrydowej aplikacji mobilnej. W przypadku wyboru innej metody do zabezpieczenia aplikacji mobilnej do zalogowania, wymagany jest kod PIN do autoryzacji zleceń.

4. Aktywacja aplikacji

Po zainstalowaniu na danym urządzeniu aplikacji hybrydowej w pierwszej kolejności aplikacja wymaga aktywacji.

Aktywacja aplikacji jest czynnością jednorazową.

Proces **aktywacji aplikacji** składa się z kilku kroków:

1. Wprowadzenie **kodu aktywacyjnego** wygenerowanego w systemie Asseco CBP/EBP.
2. Wprowadzenie **kodu SMS** przesłanego na dedykowane urządzenie.
3. Wprowadzenie oraz potwierdzenie własnego **kodu PIN**.
4. Ustawienie **metody logowania**.

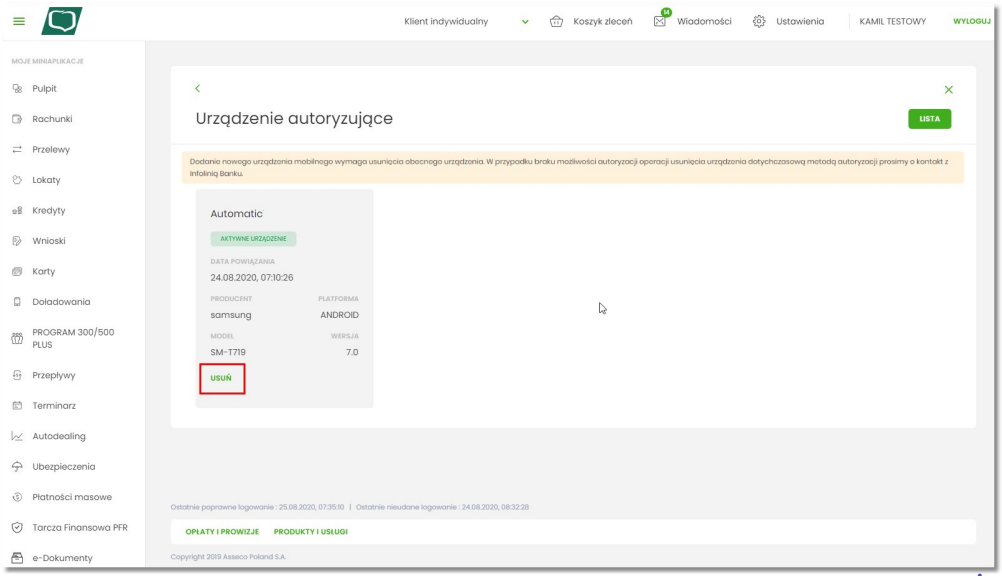
Ponowne przejście przez procedurę *aktywacji aplikacji* jest niezbędne w wyjątkowych sytuacjach:

- **zmiany urządzenia mobilnego na nowe**
  - w celu zmiany urządzenia mobilnego na nowe należy na starym urządzeniu dezaktywować aplikację, proces opisany w rozdziale **Ustawienia** → Dezaktywacja aplikacji,
  - użytkownikowi wyświetlony zostaje ekran zawierający komunikat o dezaktywacji aplikacji,

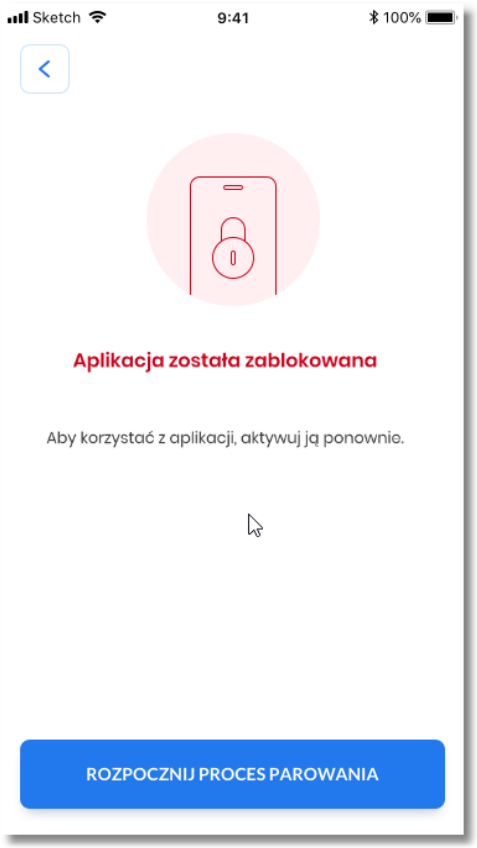
- następnie użytkownik instaluje aplikację na nowym urządzeniu i dokonuje ponownej aktywacji aplikacji.

*** zmiany sposobu autoryzacji z Asseco MAA na Aplikację Hybrydową**

- w celu zmiany metody autoryzacji należy zalogować się do systemu Asseco CBP,
- następnie należy usunąć sparowane urządzenie dla Asseco MAA i **w tej samej sesji** dodać nowe urządzenie dla Aplikacji Hybrydowej,
- usunięcie sparowanego urządzenie dla aplikacji Asseco MAA, odbywa się z pozycji menu ***Ustawienia*** → ***Urządzenie autoryzujące***, gdzie dla wyświetlonego aktywnego urządzenia wybieramy opcję **[USUŃ]**



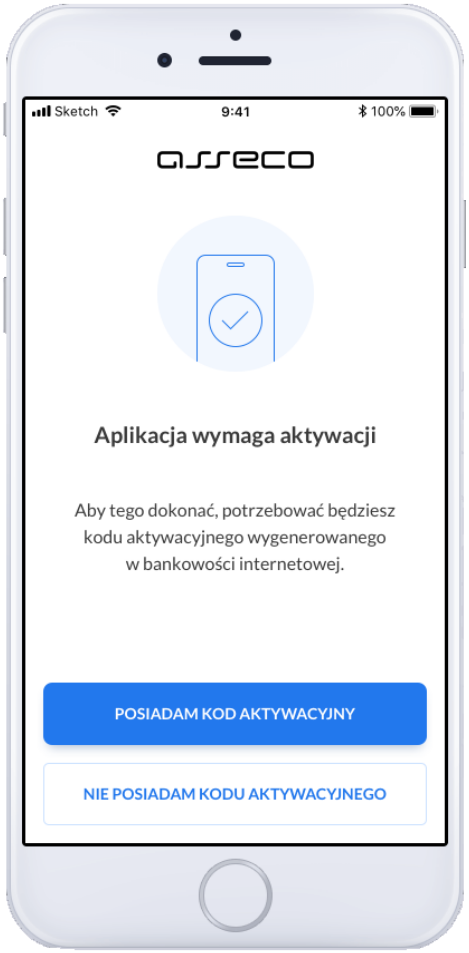
- w następnym kroku użytkownik instaluje Aplikację Hybrydową na danym urządzeniu i dokonuje ponownej aktywacji aplikacji.
    - **konieczności odblokowania dostępu do aplikacji po zablokowaniu**
- zablokowanie aplikacji, następuje gdy użytkownik poda trzykrotnie nieprawidłowy PIN w procesie autoryzacji lub autentykacji,
- użytkownikowi wyświetlona zostaje stosowna informacja z możliwością przejścia do ekranu powitalnego systemu,



- następnie użytkownik dokonuje ponownej aktywacji aplikacji.

4.1. Wprowadzenie kodu aktywacyjnego

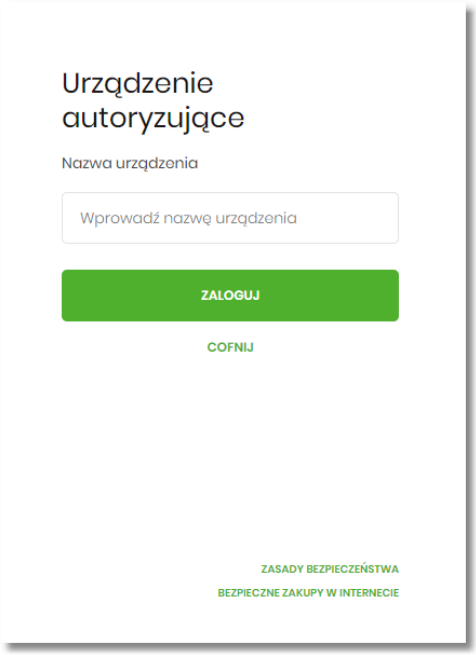
Pierwszą czynnością jaką musi wykonać użytkownik w celu aktywacji aplikacji jest wprowadzenie kodu aktywacyjnego wygenerowanego przez użytkownika w systemie Asseco CBP/EBP. Aby tego dokonać, należy wygenerować w bankowości internetowej kod aktywacyjny a następnie wybrać opcję [POSIADAM KOD AKTYWACYJNY].

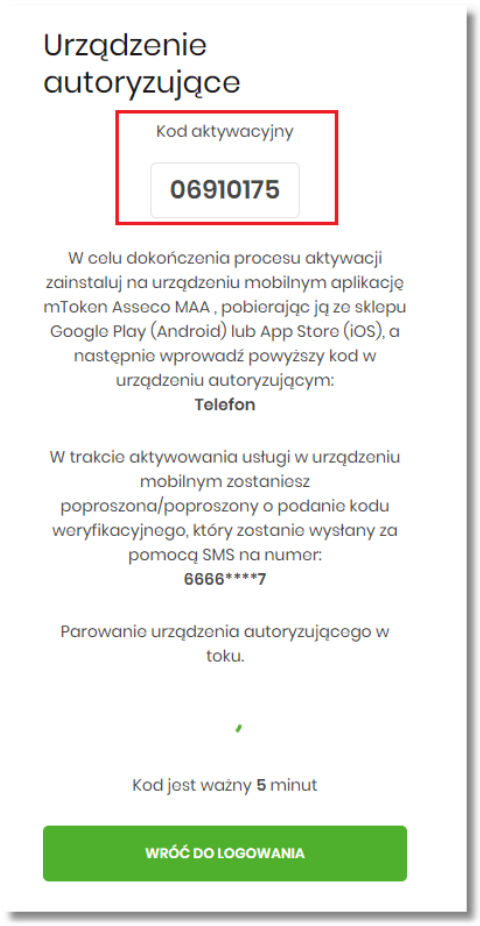


Wybranie opcji [NIE POSIADAM KODU AKTYWACYJNEGO] prezentuje użytkownikowi ekran informacyjny, z którego użytkownik ma również możliwość przejścia do kolejnego kroku aktywacji.

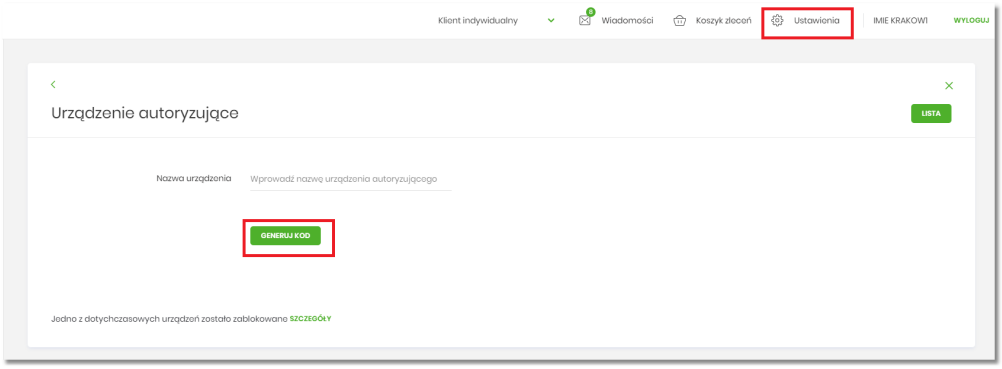
Wygenerowanie niezbędnego do aktywacji kodu odbywa sie w bankowości internetowej na dwa sposoby:

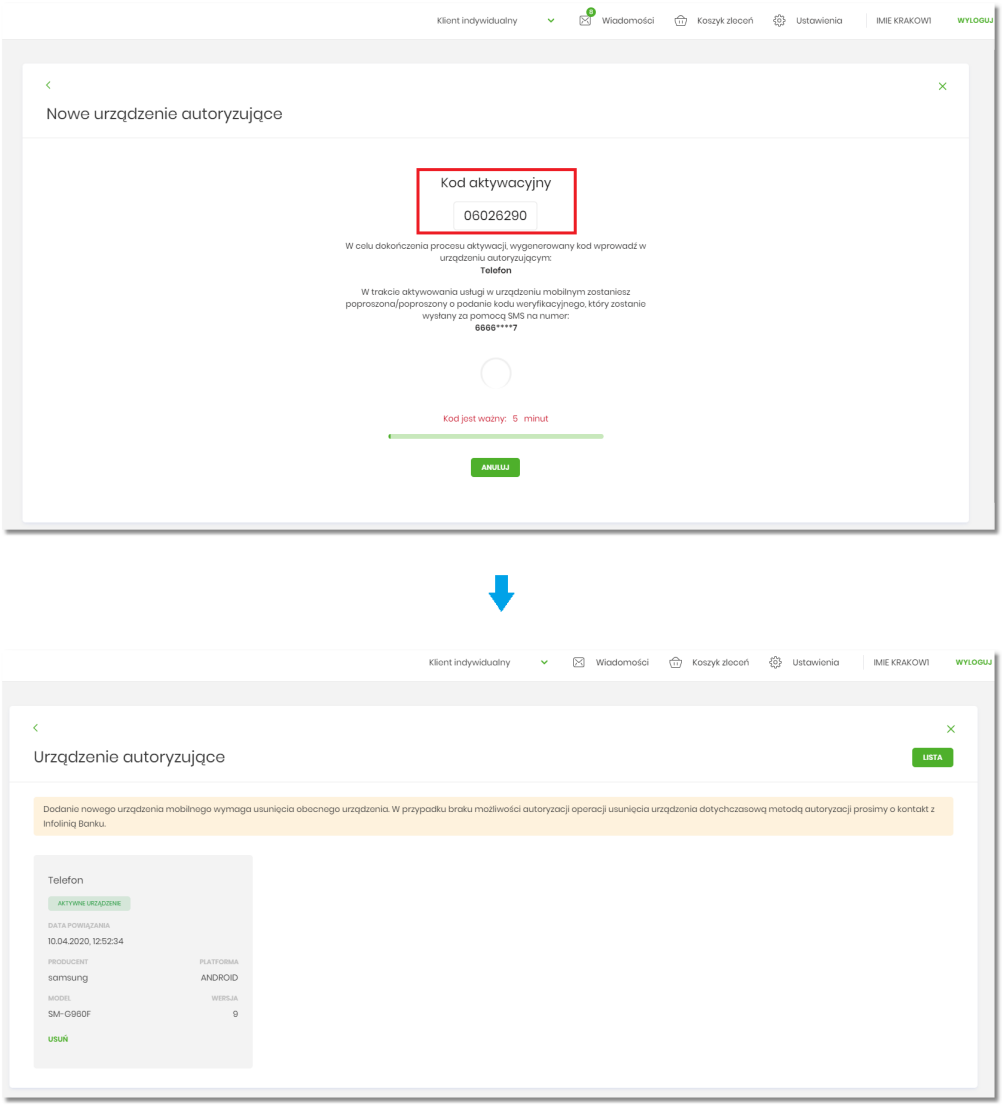
- podczas logowania, gdy użytkownik posiada włączoną autentykacje mobilna i nie posiada sparowanego urządzenia



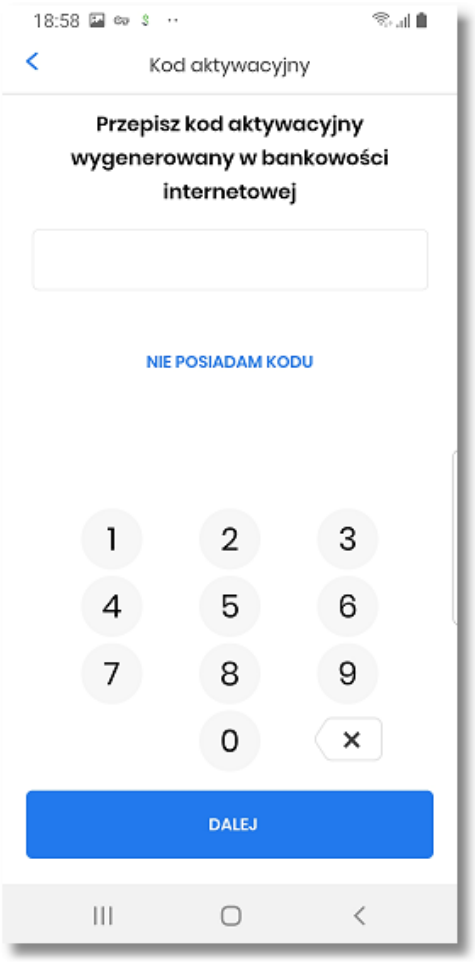


- po zalogowaniu, wybierając *Ustawienia* → *Urządzenia autoryzujące*





Po uzyskaniu kodu aktywacyjnego, użytkownikowi prezentowany jest ekran do wpisania kodu aktywacyjnego. Przycisk z ikonką × powoduje wyczyszczenie wcześniej wprowadzonego znaku w polu. Po kliknięciu w Link [NIE POSIADAM KODU], użytkownikowi wyświetlany jest ekran informacyjny jak we wcześniejszym kroku. W celu zatwierdzenia wpisanego kodu aktywacyjnego należy wybrać przycisk [DALEJ].



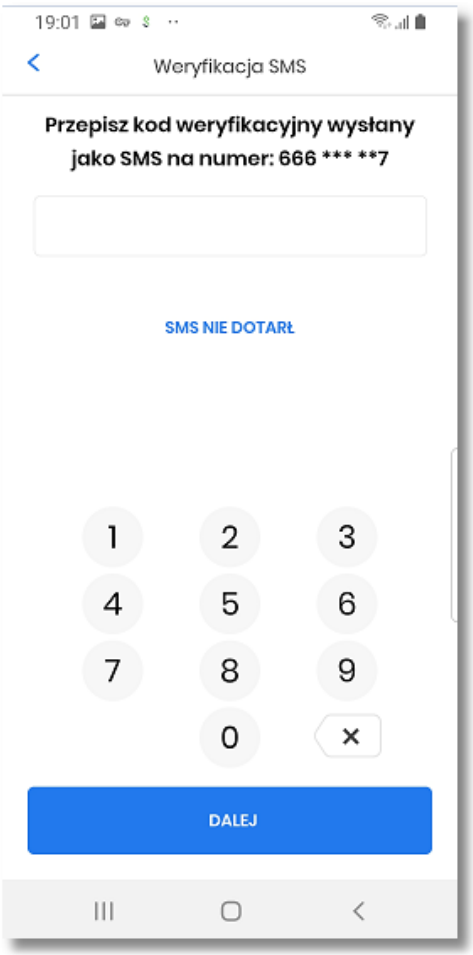
System weryfikuje poprawność wprowadzonego kodu aktywacyjnego w przypadku braku zgodności użytkownikowi wyświetlany jest komunikat.

W górnej części formularza **Kod aktywacyjny** dostępny jest przycisk:

-  - umożliwiający powrót do ekranu powitalnego.

4.2. Wprowadzenie kodu SMS

W kolejnym kroku na formularzu **Weryfikacja SMS** w celu identyfikacji należy wprowadzić dodatkową informację zgodnie z instrukcją wyświetlaną na ekranie. Informacją dodatkową jest kod weryfikacyjny wysłany za pomocą wiadomości SMS. Po wprowadzeniu (za pomocą klawiatury na urządzeniu) danych w polu **Weryfikacja SMS** należy w celu zatwierdzenia wybrać ponownie przycisk [DALEJ].



W górnej części formularza **Weryfikacja SMS** dostępny jest przycisk:

-  - umożliwiający powrót do poprzedniego kroku aktywacji.

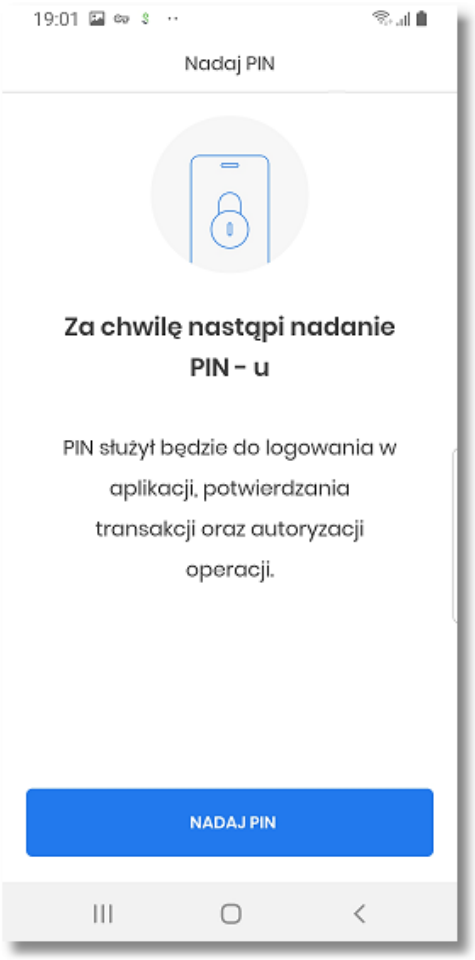
W przypadku nie otrzymania kodu SMS i wybraniu opcji [SMS NIE DOTARŁ], zostanie użytkownikowi wyświetlony poniższy komunikat wraz z możliwością ponownego procesu aktywacji po wybraniu przycisku [ROZPOCZNIJ PROCES PONOWNIE]

W górnej części formularza **Weryfikacja SMS** dostępny jest przycisk:

-  - umożliwiający wyjście z komunikatu.

4.3. Wprowadzenie kodu PIN

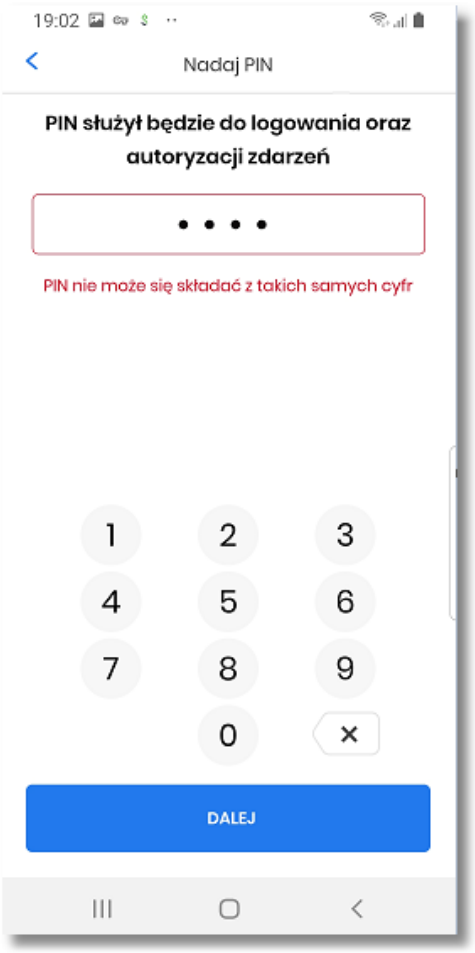
Po prawidłowej weryfikacji kodu wysłanego jako SMS, użytkownikowi wyświetlana jest informacja o kolejnym kroku jakim jest nadanie PIN-u, służącego do logowania w aplikacji, potwierdzania transakcji oraz autoryzacji operacji. Użytkownik zatwierdza decyzję poprzez przycisk [NADAJ PIN].



W następnym kroku w polu **Nadaj PIN** należy wprowadzić kod PIN, który będzie służył do logowania w aplikacji oraz wybrać przycisk [DALEJ].

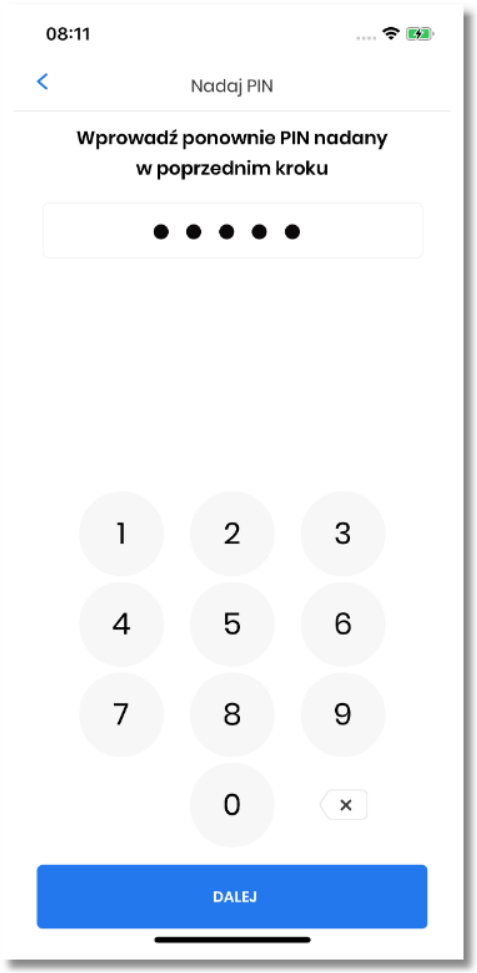
Kod PIN musi posiadać minimum 5 a maksymalnie 8 znaków.

Dodatkowo w procesie nadawania kodu PIN aplikacja weryfikuje wprowadzanie prostych haseł takich jak 11111, 22222, 123123, 12345. W przypadku zdefiniowania takiej kombinacji cyfr w systemie zostanie zaprezentowany komunikat walidacyjny.

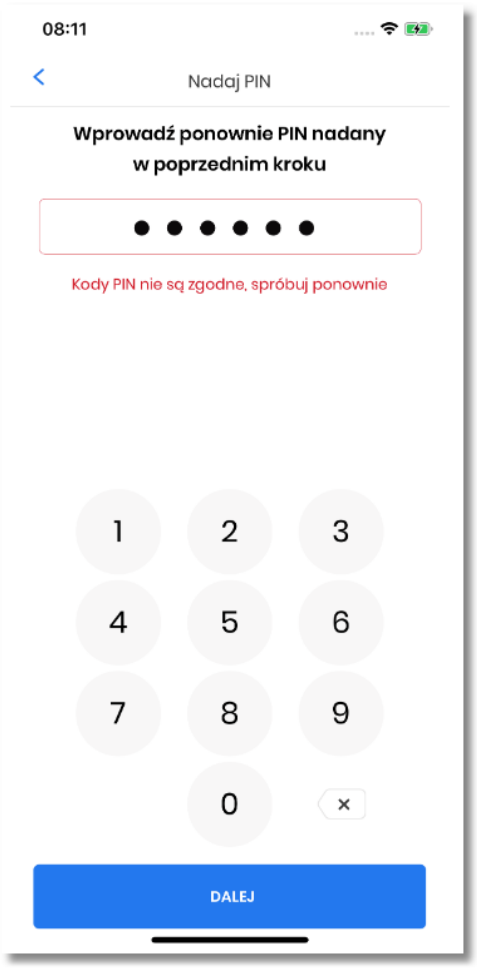

19:02
Nadaj PIN
PIN służył będzie do logowania oraz autoryzacji zdarzeń
PIN nie może się składać z takich samych cyfr
1
2
3
4
5
6
7
8
9
0
DALEJ

Po podaniu prawidłowej kombinacji cyfr stanowiącej unikalny identyfikator użytkownika, system informuje o tym odpowiednim komunikatem.

W kolejnym kroku należy ponownie wprowadzić kod PIN w polu **Potwierdź PIN** i zatwierdzić poprzez przycisk [DALEJ].



System kontroluje prawidłowość i zgodność kodu PIN zdefiniowanego w polach Nowy PIN oraz Potwierdź PIN.



W górnej części formularza **Nadaj PIN** dostępny jest przycisk:

-  - umożliwiający powrót do poprzedniego ekranu.

4.4. Ustawienie metody logowania

Po prawidłowym nadaniu PIN-u, system umożliwia użytkownikowi ustawienie metody logowania.

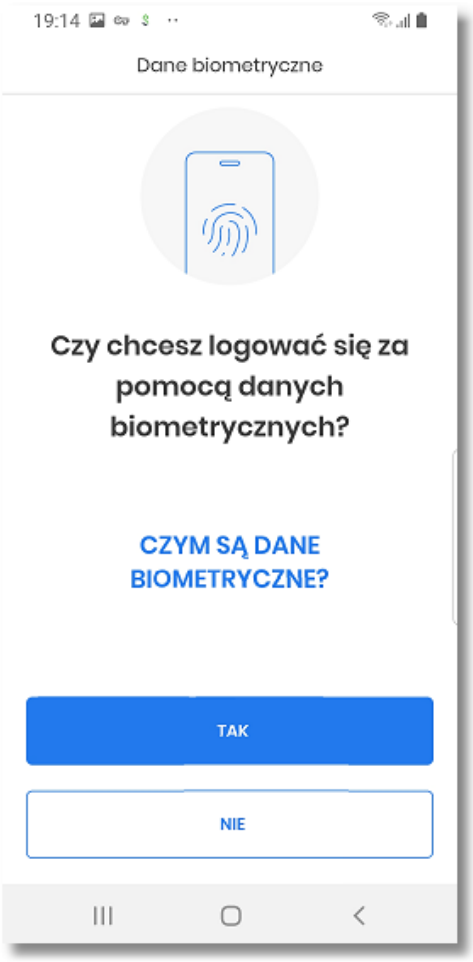
Metody logowania udostępniane przez system to:

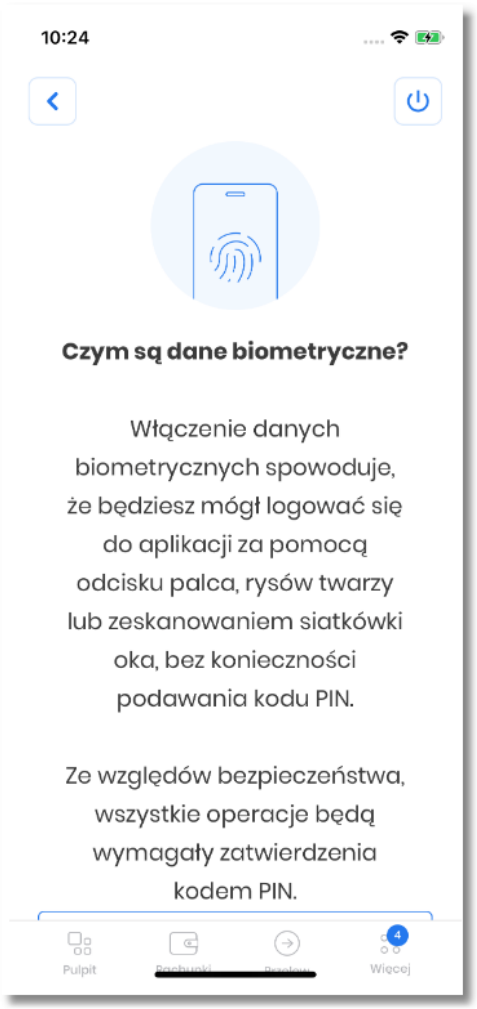
- Kod PIN - dla systemu android oraz iOS,
- metody biometryczne:
  - Odcisk palca - dla systemu android oraz iOS,
  - Face Id - dla systemu iOS,

Opcja 'Odcisk palca' oraz 'Face Id' może być wybrana, gdy urządzenie zostało uprzednio skonfigurowane do takiej obsługi.

W celu wyboru metody system prezentuje formularz **Dane biometryczne** udostępniający zestaw akcji:

- [CZYM SĄ DANE BIOMETRYCZNE] - umożliwia wyświetlenie użytkownikowi komunikatu informacyjnego,
- [TAK] – umożliwia włączenie metody biometrycznej w procesie logowania:
- [NIE] – umożliwia rezygnacje z metody biometrycznej, tym samy logowanie do aplikacji hybrydowej odbywać się będzie przy pomocy ustawionego kodu PIN,



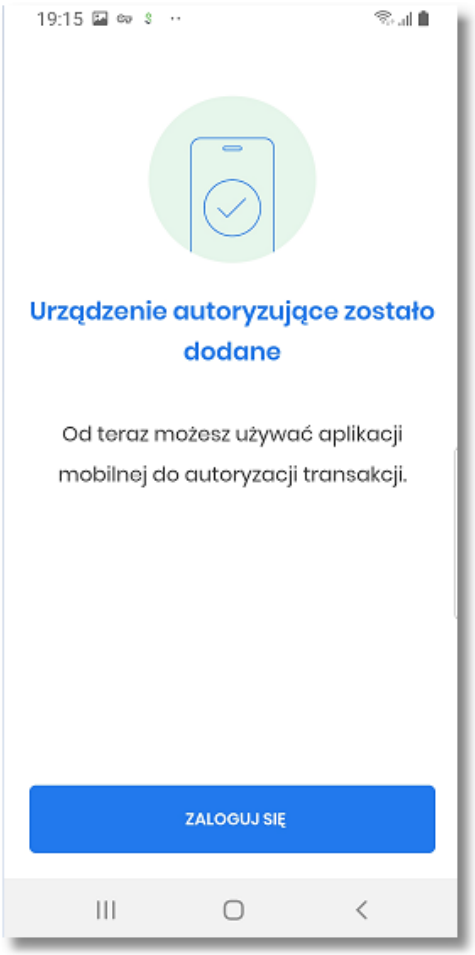


W górnej części formularza prezentującego informacje o danych biometrycznych dostępny jest przycisk:

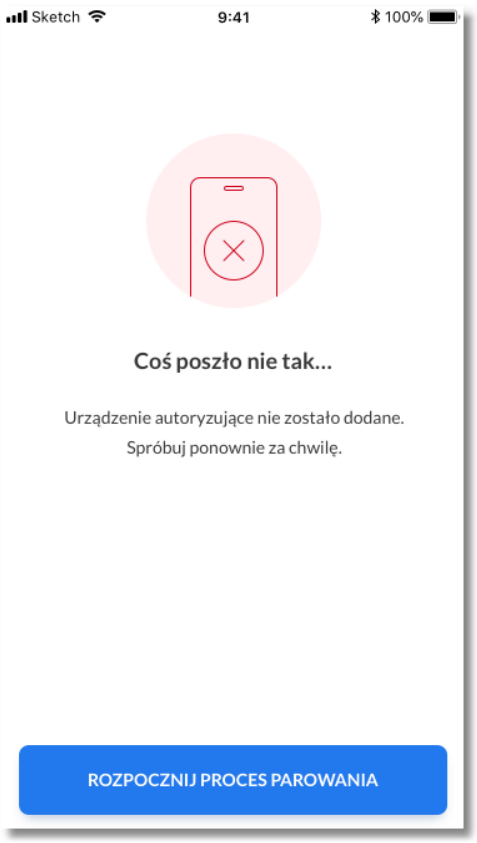
-  - umożliwiający powrót do poprzedniego ekranu,
-  - umożliwiający wylogowanie oraz powrót do ekranu powitalnego.

Szczegółowe informacje dotyczące danych biometrycznych zostały opisane w rozdziale **Ustawienia → *Dane biometryczne***.

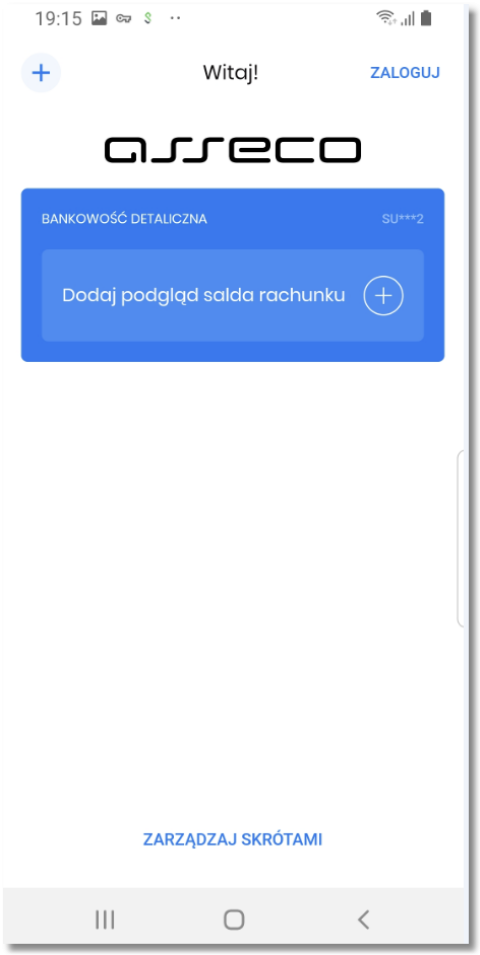
Po dokonaniu aktywacji aplikacji i ustaleniu sposobu logowania za pomocą PIN-u lub danych biometrycznych, użytkownikowi wyświetlany jest ekran informujący o dodaniu urządzenia autoryzującego, umożliwiającego zalogowanie się w aplikacji hybrydowej wybierając przycisk [ZALOGUJ SIĘ].



W przypadku niepowodzenia aktywacji aplikacji, użytkownikowi również wyświetlany jest odpowiedni komunikat.



Po udanym procesie aktywacji aplikacji i zalogowaniu użytkownika w aplikacji hybrydowej , wyświetlany jest ekran główny aplikacji.


19:15
Witaj!
ZALOGUJ
BANKOWOŚĆ DETALICZNA
SU***2
Dodaj podgląd salda rachunku
ZARZĄDZAJ SKRÓTAMI

5. Logowanie

W celu zalogowania się do Asseco Aplikacja hybrydowa należy w pierwszym kroku dokonać *aktywacji aplikacji*. Jest to jednorazowa czynność, po wykonaniu której, użytkownik będzie mógł sie już logować za pomocą wybranej metody.

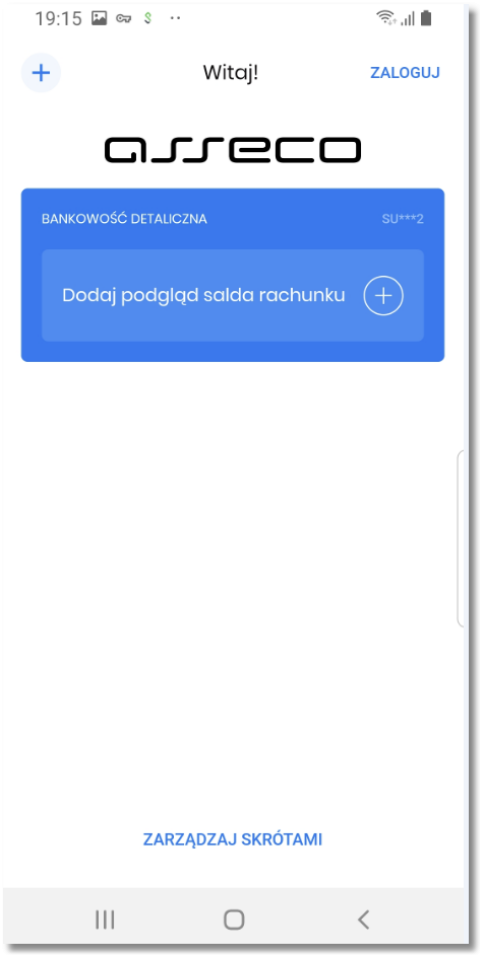
Proces logowania użytkownika do hybrydowej aplikacji mobilnej, składa się z następujących kroków:

1. Użytkownik uruchamia aplikację na urządzeniu mobilnym. Wyświetlany jest ekran powitalny.
2. Użytkownik loguje się dowolną metodą autentykacji, wybraną podczas procesu aktywacji.
3. Aplikacja hybrydowa prezentuje pulpit w kontekście zalogowanego użytkownika.

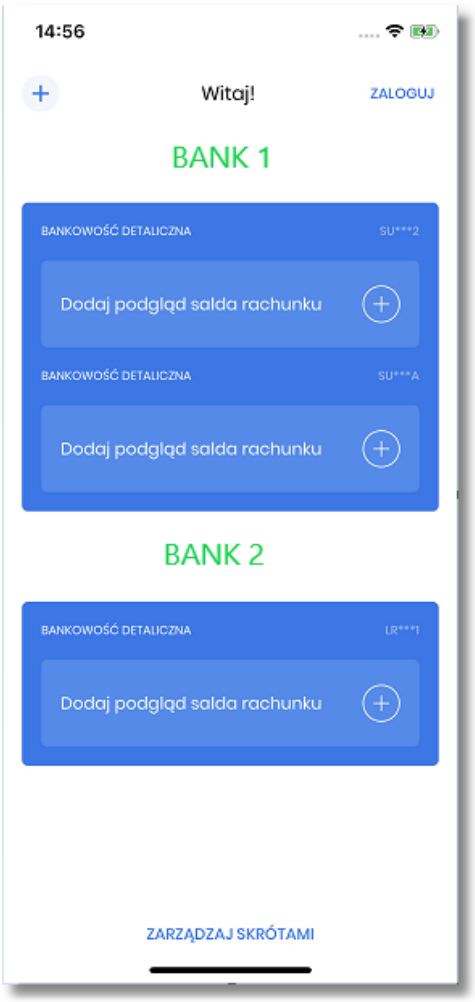
5.1. Logowanie - Ekran powitalny

W pierwszym kroku logowania użytkownikowi wyświetlany jest ekran powitalny, zawierający:

- sekcję aktywowanego użytkownika:
  - nazwa jednostki Banku
  - częściowo zamaskowany login użytkownika
  - [50] [Dodaj podgląd salda rachunku] - umożliwia przejście do strony zarządzania skrótami pozwalającej zdefiniować rodzaj (kwota, procent) wyświetlanego salda dla wybranego rachunku (Ustawienia → Zarządzanie skrótami → Dostępne środki - Włącz skrót)
- akcje:
  -  [DODAJ] - umożliwia przejście do pierwszego kroku aktywacji aplikacji dla kolejnego użytkownika lub kolejnej bankowości (Aktywacja → Kod aktywacyjny),
  -  [ZALOGUJ] - umożliwia przejście do strony logowania do aplikacji i następnie wyświetlenie użytkownikowi PULPITU,
  -  [ZARZĄDZAJ SKRÓTAMI] - umożliwia przejście do strony logowania do aplikacji i następnie wyświetlenie użytkownikowi (Ustawienia → Zarządzanie skrótami).

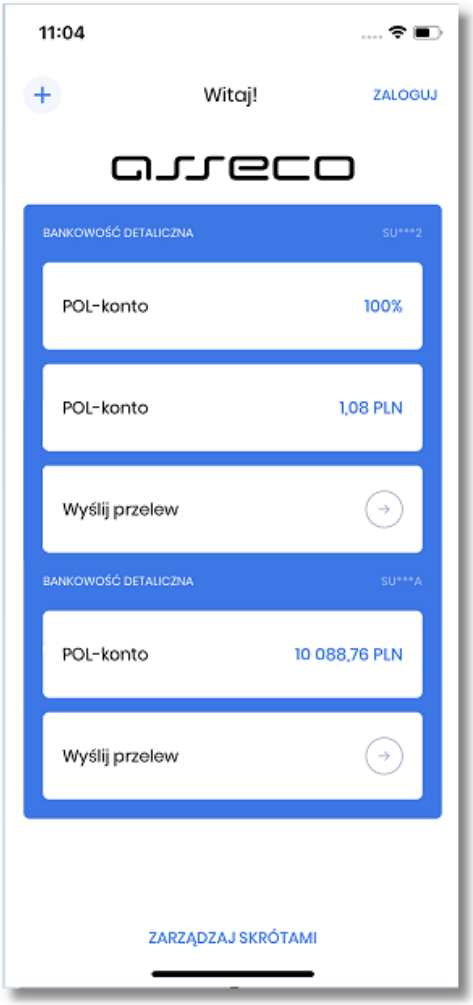


Po wybraniu opcji [DODAJ] użytkownik ma możliwość aktywowania dowolnej liczby użytkowników na jednym urządzeniu w ramach różnych systemów bankowych.



W przypadku opcji [ZALOGUJ] oraz [ZARZĄDZAJ SKRÓTAMI] jeśli użytkownik aplikacji aktywował wiecej niż jednego użytkownika bankowości internetowej na danym urządzeniu, w takim przypadku konieczne jest wybranie użytkownika w kontekście którego zostanie zalogowany.

Jeśli użytkownik dokonał konfiguracji ekranu powitalnego *Zarządzanie skrótami* to apliakcja prezentuje informacje o dostepnych środkach na wybranym rachunku, w postaci kwoty lub procent.



Poniżej wyświetlana jest dodatkowa akcja:

[Wyślij przelew] - prowadząca do strony realizacj przelewu (Przelewy → Przelew zwykły), po wcześniejszym zalogowaniu do aplikacji.

5.2. Logowanie - Metoda autentykacji

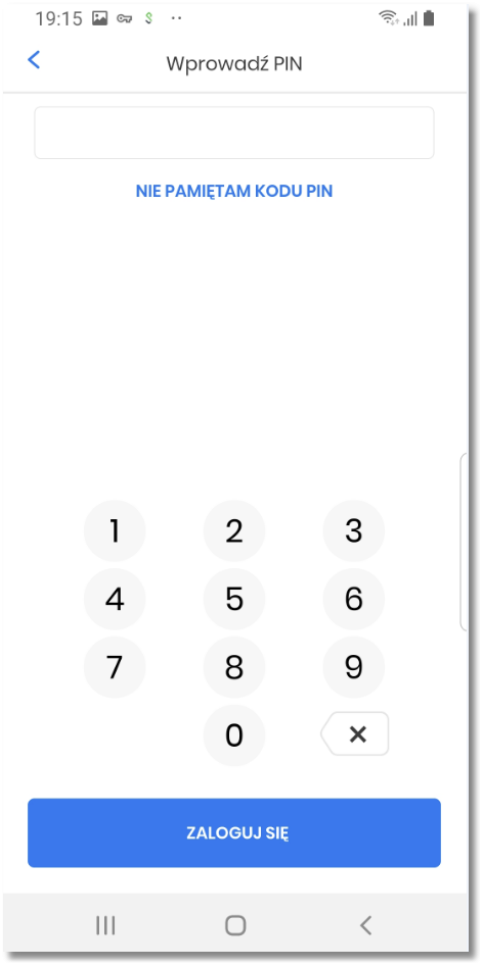
Dostęp do hybrydowej aplikacji mobilnej zabezpieczony jest dowolną metodą wybraną przez użytkownika:

- kod PIN,
- metoda biometryczna:
  - 'Odcisk palca',
  - 'Face ID' - tylko dla urządzeń z systemem iOS.

Wybór na ekranie powitalnym opcji [ZALOGUJ], [ZARZĄDZAJ SKRÓTAMI] czy [Dodaj podgląd salda rachunku] pozwala na przejście do kolejnego kroku logowania, w którym należy wprowadzić kod PIN nadany przez użytkownika w procesie aktywacji.

5.2.1. Logowanie przy użyciu 'kodu PIN'

W drugim kroku logowania użytownikowi wyświetlany jest formularz **Wprowadź PIN** pozwalający na zalogowanie się wybraną metodą autentykacji, potwierdzany przyciskiem [ZALOGUJ SIĘ].



Poniżej pola do wprowadzenia PIN-u wyświetlany jest Link 

[NIE PAMIETAM KODU PIN], który po wybraniu prezentuje ekran informacyjny oraz przycisk do ponownego rozpoczęcia procesu parowania urządzenia.

Użytkownik na formularzu **Wprowadź PIN** wpisuje dane. Aplikacja weryfikuje poprawność wprowadzonych danych.

Aplikacja zabezpieczona jest przed wielokrotnym wprowadzeniem błędnego kodu PIN. Po przekroczeniu sparametryzowanej liczby błędnie wprowadzonych kodów PIN użytkownikowi zostanie zaprezentowany komunikat informacyjny o dezaktywacji aplikacji. W takim przypadku, konieczne będzie ponowne powiązanie urządzenia mobilnego z systemem bankowości internetowej.

W lewej części górnego menu formularza **Wprowadź PIN** dostępny jest przycisk:

-  - umożliwiający powrót do wyświetlenego wcześniej formularza ekranu powitalnego.

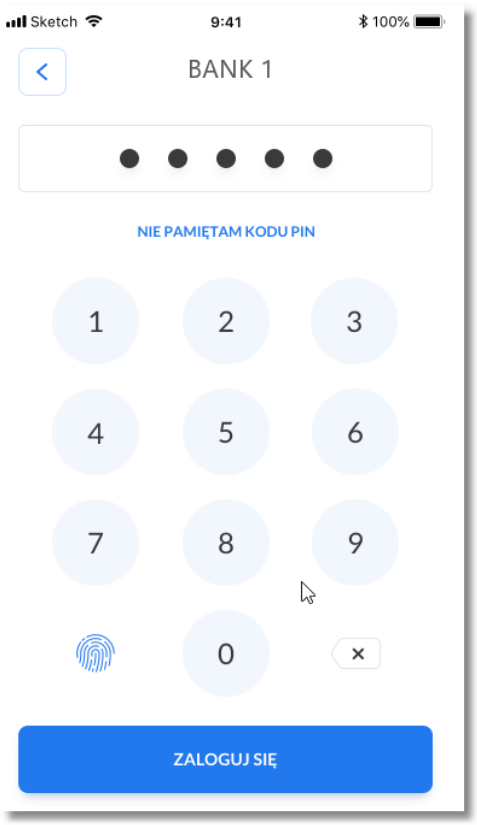
W prawej części górnego menu formularza **Nie pamiętam kodu PIN** dostępny jest przycisk:

-  - umożliwiający zamknięcie komunikatu i wyświetlenie wcześniejszego formularza.

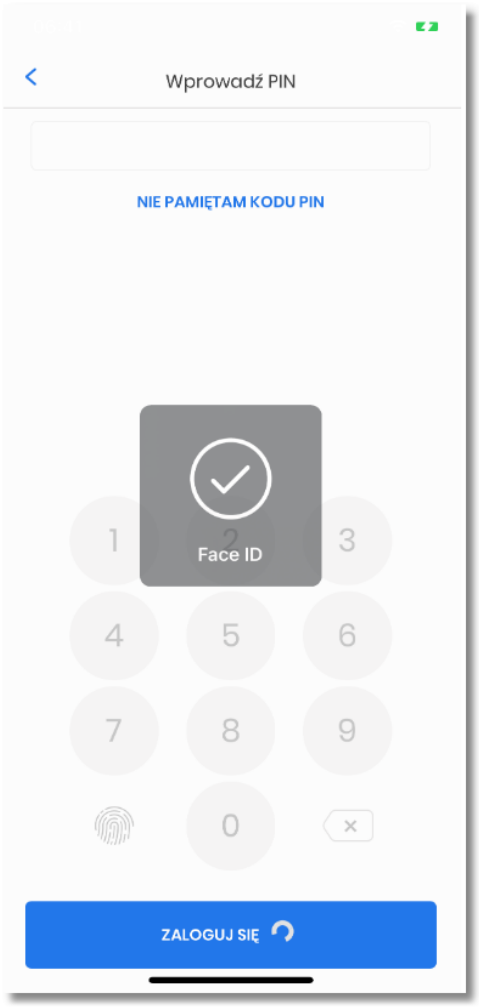
5.2.2. Logowanie przy użyciu metody biometrycznej

W procesie logowania do aplikacji zostały użyte natywne sprzętowe funkcje urządzeń mobilnych, co oznacza, że logowanie z użyciem ***Odcisku palca*** czy ***Face ID*** użytkownika dostępna jest tylko na urządzeniach posiadających takie funkcjonalnościi po wcześniejszym ich skonfigurowaniu.

Wybór w prawym górnym rogu opcji [ZALOGUJ] pozwala na przejście do pierwszego kroku logowania, w którym należy wprowadzić kod PIN nadany przez użytkownika w procesie aktywacji urządzenia a następnie wybrać przycisk [ZALOGUJ SIĘ]. W przypadku wybrania w procesie aktywacji metody biometrycznej, dodatkowo wyświetlana jest ikonka pozwalajaca na identyfikacje wybranym typem biometrii  .



W procesie logowania za pomocą *Face ID* system bezpośrednio rozpoznaje twarz i loguje użytkownika.



W procesie logowania za pomocą *odcisku palca* system wyświetla dodatkowe okno informacyjne z prośbą o autentykacje odciskiem palca, a po prawidłowej weryfikacji użytkownik zostaje zalogowany do apliakcji.

System kontroluje prawidłowość danych biometrycznych. W przypadku nieprawidłowej weryfiakcji, użytkownik zostaje poinformowany stosownym komunikatem.

Logowanie za pomocą kodu PIN, odcisku palca czy Face ID jest definiowana w procesie aktywacji apliakcji lub w każdej chwili z poziomu ustawień aplikacji mobilnej (Więcej → Ustawienia → Dane biometryczne). Opcja logowania przy użyciu 'odcisku palca' może być wybrana, gdy urządzenie zostanie uprzednio skonfigurowane do takiej obsługi (to oznacza na przykład, że brak dodanego odcisku palca uniemożliwi odblokowywanie aplikacji odciskiem palca).

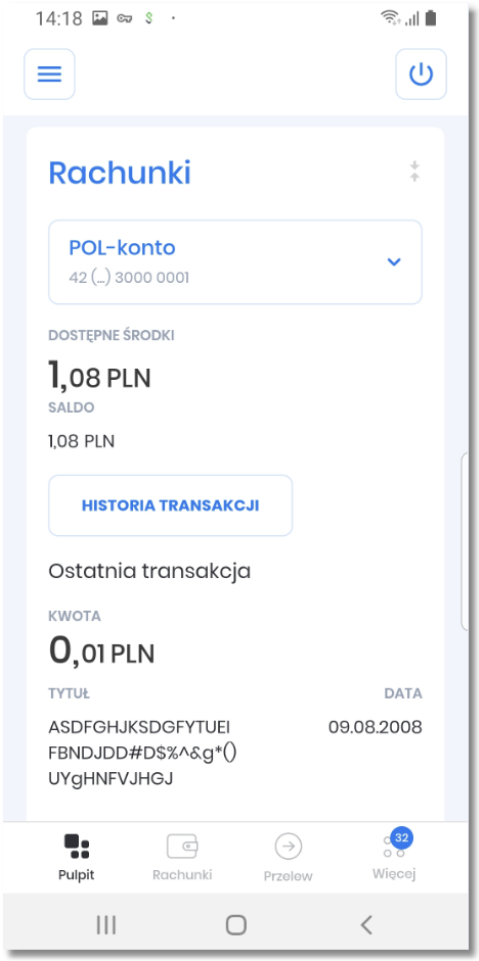
5.2.3. Prezentacja pulpitu po zalogowaniu

Po zalogowaniu użytkownik uzyskuje pełen dostęp do funkcjonalności:

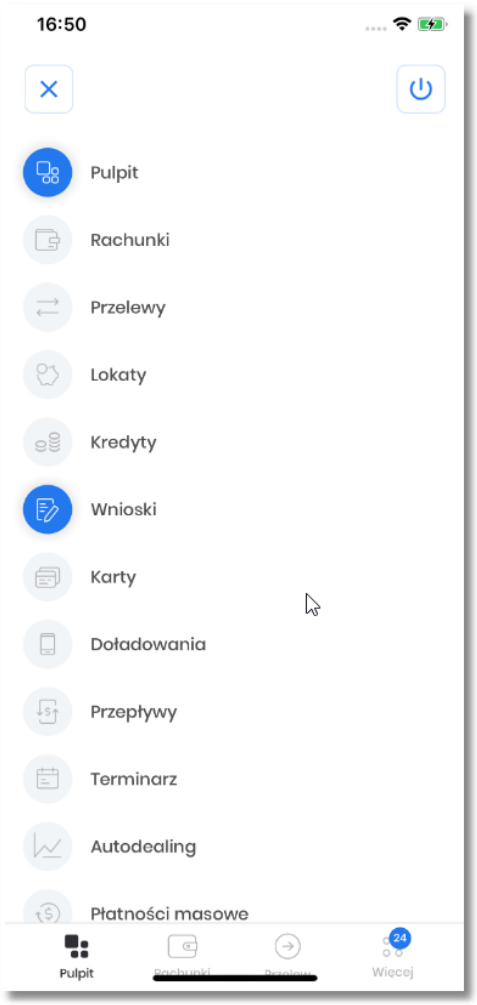
- bankowości internetowej **Asseco CBP/EBP**,
- wbudowanej aplikacji **Asseco MAA** służącej do autoryzacji dyspozycji oraz logowania,
- zarządzania **aplikacją hybrydową**.

Aplikacja hybrydowa posiada następujące różnice pomiędzy wersją bankowości internetowej **Asseco CBP/EBP** a aplikacją mobilną: * usunięty został eksport historii operacji do XML * zmieniony został ekran autoryzacji - w momencie kiedy użytkownik ma ustawioną metodę autoryzacji MAA, wyświetlany jest wkran z komuniaktem'Wymagane potwierdzenie PINem' * zablkowane zostały wszystkie importy.

Użytkownikowi wyświetlany jest ***Pulpit*** zawierający funkcjonalności systemu CBP/EBP.

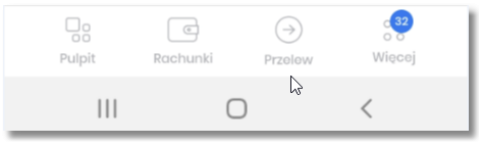


Za pomocą ikonki  , użytkownikowi wyświetlane jest ***boczne menu*** pozwalające na korzystanie z funkcjonalności systemu CBP/EBP.



Poniżej wyświetlane jest ***menu dolne***, pozwalające na szybki dostęp do:

- **Pulpitu**,
- **Rachunków**,
- **Przelewów**,
- **Więcej**.

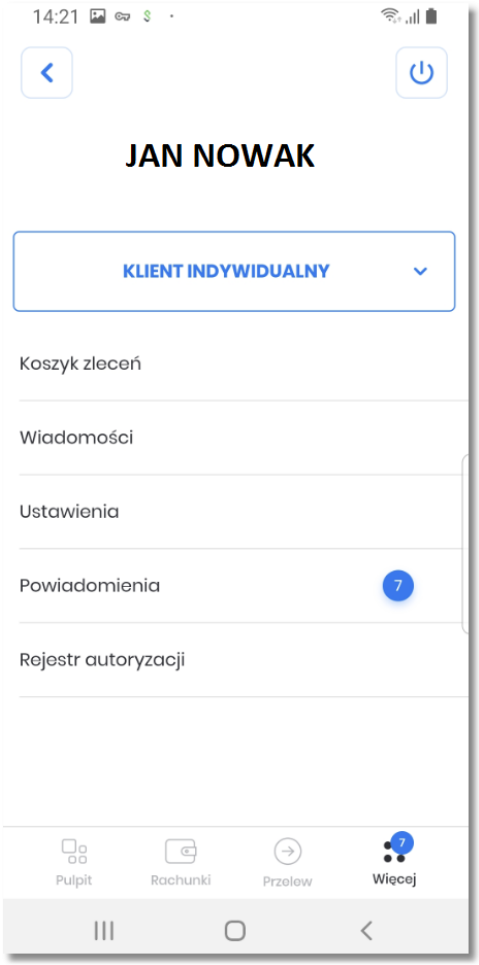


Wybierając menu **Pulpit**, **Rachunki** czy **Przelewy** użytkownikowi udostępniana jest funkcjonalność, która odpowiada posiadanemu dostępowi do miniaplikacji w systemie Asseco CBP/EBP, po wyborze odpowiedniego kontekstu.

Wybierając menu **Więcej** użytkownik uzyskuje dostęp do funkcjonalności:

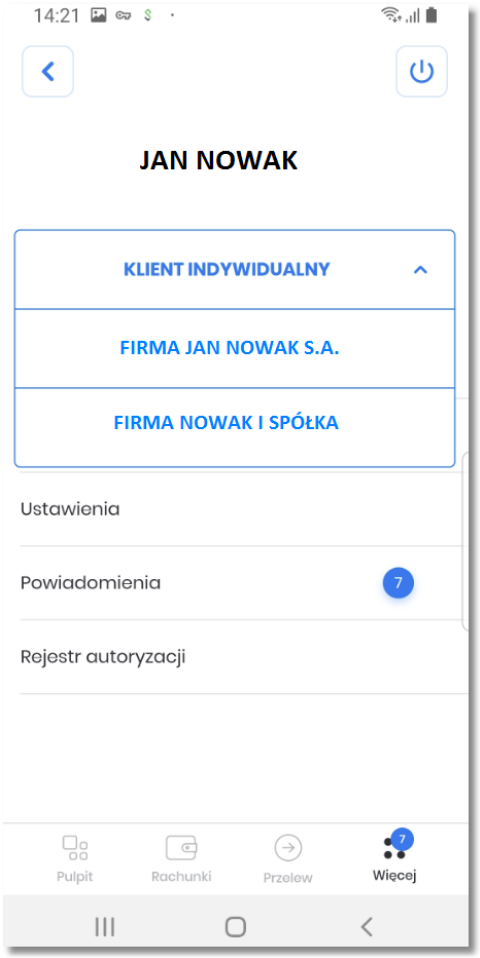
- **Koszyk zleceń**,

- **Wiadomości**,
- **Ustawienia**, moduł zawierający nowe funkcjonalności *Ustawienia*,
- **Powiadomienia**, moduł zawierający nowe funkcjonalności *Powiadomienia*,
- **Rejestr autoryzacji**, moduł zawierający nowe funkcjonalności *Rejestr autoryzacji*,

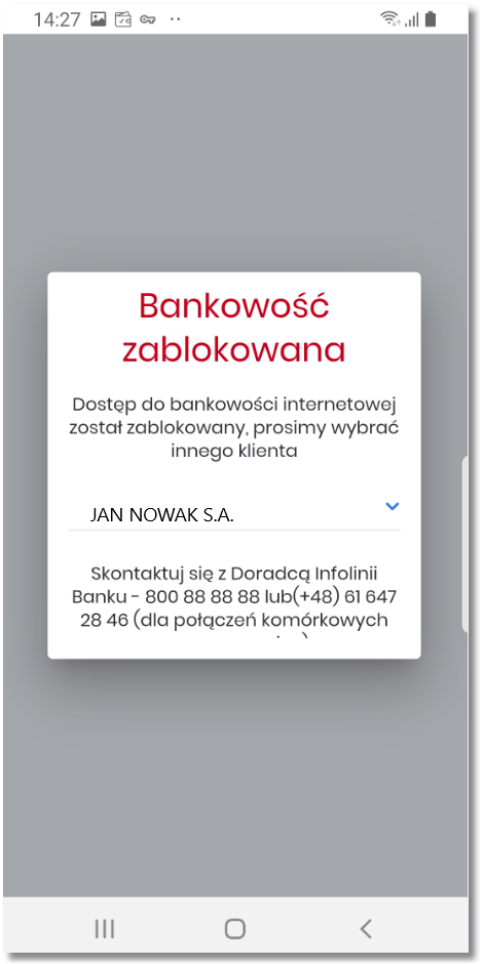


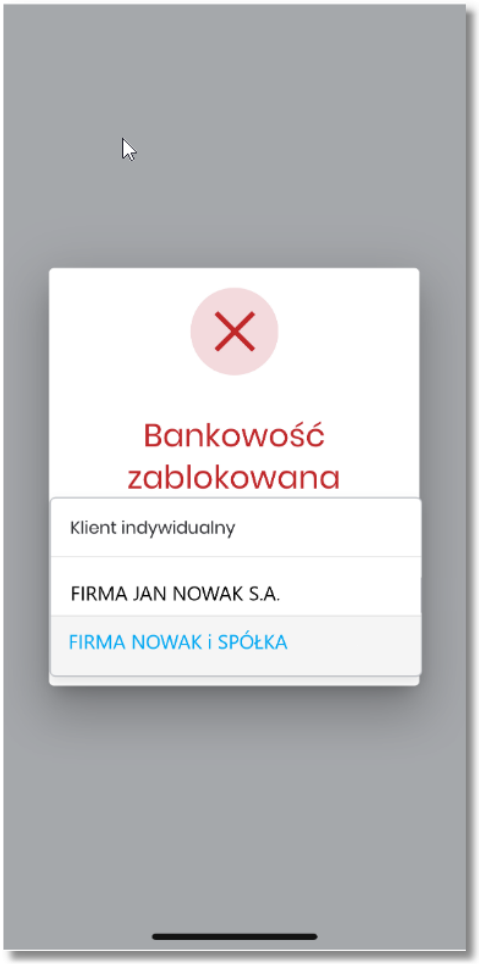
Wybierając menu **Koszyk zleceń** lub **Wiadomości** użytkownikowi udostępniana jest funkcjonaloność, która odpowiada posiadanemu dostępowi do miniaplikacji w systemie Asseco CBP/EBP, po wyborze odpowiedniego kontekstu.

Dodatkowo nad menu wyświetlana jest nazwa domyślnego **kontekstu użytkownika** w którym został zalogowany. Poniżej znajduje się lista wszystkich kontekstów użytkownika, zarówno detaliczny jak i firmowych. Użytkownik ma możliwość zmiany kontekstu na dowolny poprzez wybranie z listy. Aplikacja automatycznie wyświetli pulpit z danymi wybranego kontekstu.



W momencie wyboru przez użytkownika innego kontekstu z listy, system sprawdza czy kontkest jest dostępny. W przypadku gdy dany kontekst jest zablokowany, użytkownikowi wyświetlany jest odpowiedni komunikat zawierający także listę kontekstów pozwalającą na powrót do innego aktywnego kontekstu.


14:27
Bankowość zablokowana
Dostęp do bankowości internetowej został zablokowany, prosimy wybrać innego klienta
JAN NOWAK S.A.
Skontaktuj się z Doradcą Infolinii Banku - 800 88 88 88 lub(+48) 61 647 28 46 (dla połączeń komórkowych


Bankowość zablokowana
Klient indywidualny
FIRMA JAN NOWAK S.A.
FIRMA NOWAK i SPÓŁKA

6. Autoryzacja dyspozycji

Autoryzacja dyspozycji w aplikacji hybrydowej realizowana jest za pomocą ustawionego w procesie aktywacji aplikacji kodu PIN.

Autoryzacji dyspozycji w aplikacji hybrydowej obejmuje:

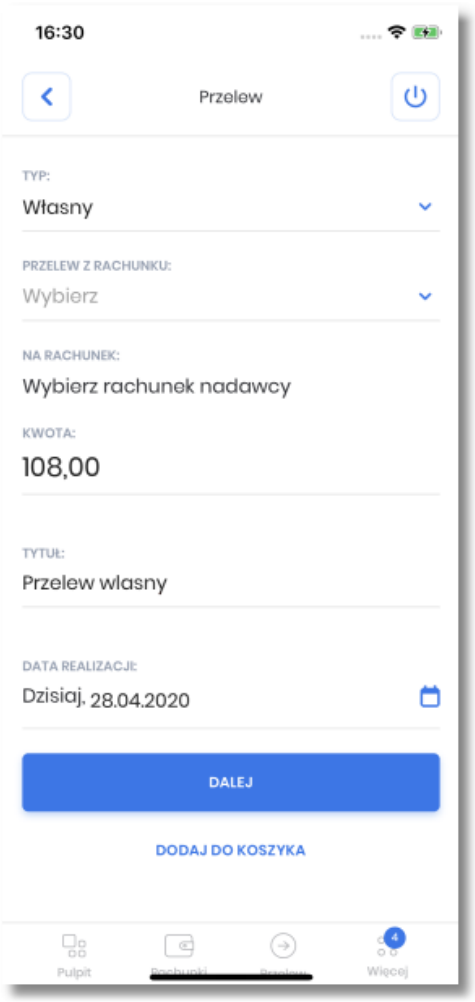
- autoryzację dyspozycji złożonych w aplikacji hybrydowej korzystających z funkcjonalności systemu CBP/EBP, dyspozycje **definiowane wewnątrz** aplikacji hybrydowej,
- autoryzację dyspozycji złożonych z poziomu aplikacji webowej systemu CBP/EBP, autoryzowane w aplikacji hybrydowej przychodzące **przed zalogowaniem** użytkownika w aplikacji hybrydowej na urządzeniu mobilnym,
- autoryzację dyspozycji złożonych z poziomu aplikacji webowej systemu CBP/EBP, autoryzowane w aplikacji hybrydowej przychodzące **po zalogowaniu** użytkownika w aplikacji hybrydowej na urządzeniu mobilnym.

6.1. Autoryzacja dyspozycji składanej *wewnątrz* aplikacji hybrydowej

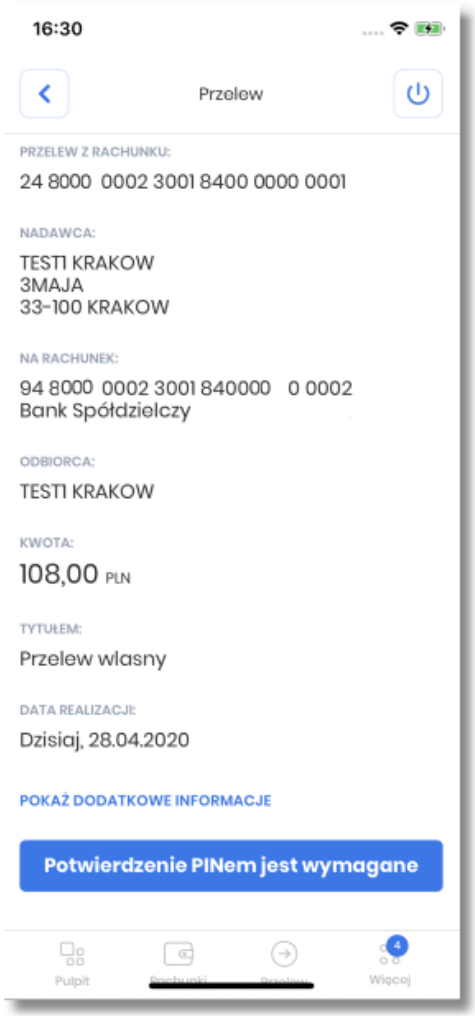
Dyspozycje definiowane w aplikacji hybrydowej (wewnętrzne), wykorzystują funkcjonalność systemu internetowego Asseco CBP/EBP oraz Asseco MAA.

Przykładowa funkcjonalność złożenia zlecenia przebiega w 4 krokach:

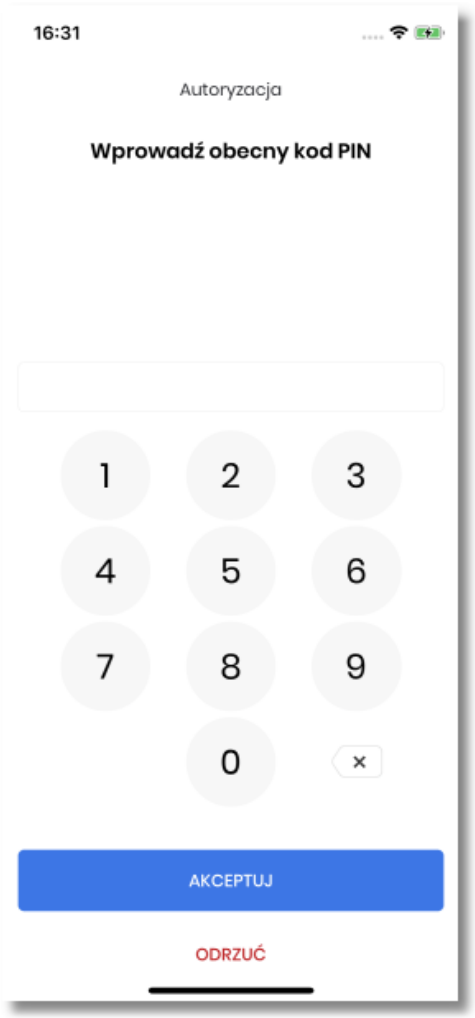
1. Złożenie zlecenia



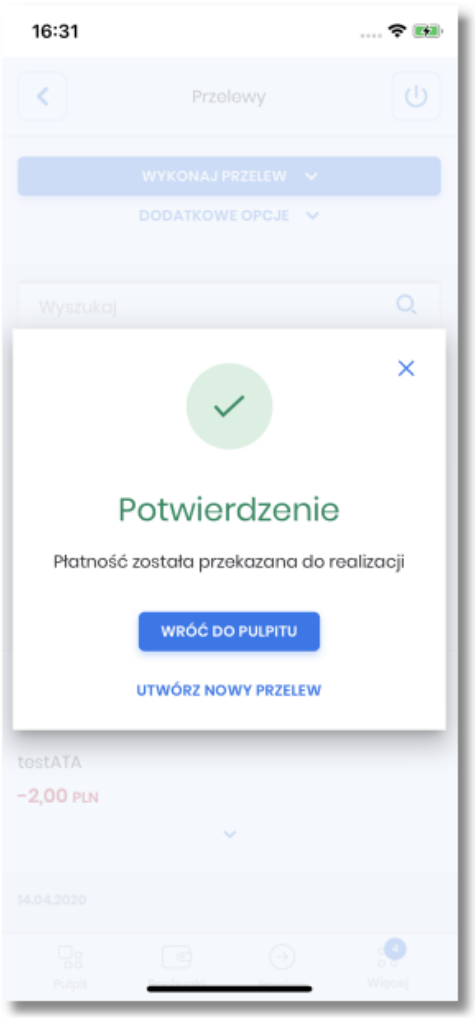
2. Prezentacja szczegółów składanego zlecenia



3. Autoryzacja składanego zlecenia



4. Status złożonego zlecenia



Autoryzacja zleceń w aplikacji mobilnej realizowana jest za pomocą kodu PIN.

Autoryzacja zleceń składanych w aplikacji hybrydowej zachowuje wszelkie założenia i walidacje autoryzacyjne funkcjonalności systemu internetowego Asseco CBP/EBP.

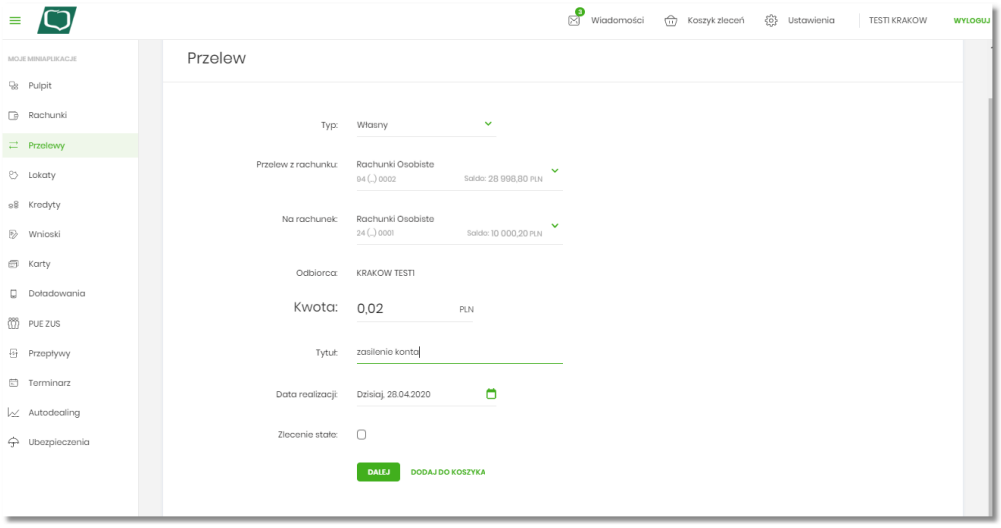
6.2. Autoryzacja dyspozycji zewnętrznej przychodzącej *przed zalogowaniem*

Aplikacja mobilna posiada zintegrowany moduł Asseco MAA, dzięki czemu dla użytkowników bankowości elektronicznej Asseco CBP aplikacja hybrydowa dostarcza funkcjonalność tokena mobilnego dla autoryzacji transakcji dokonywanych z poziomu aplikacji internetowej.

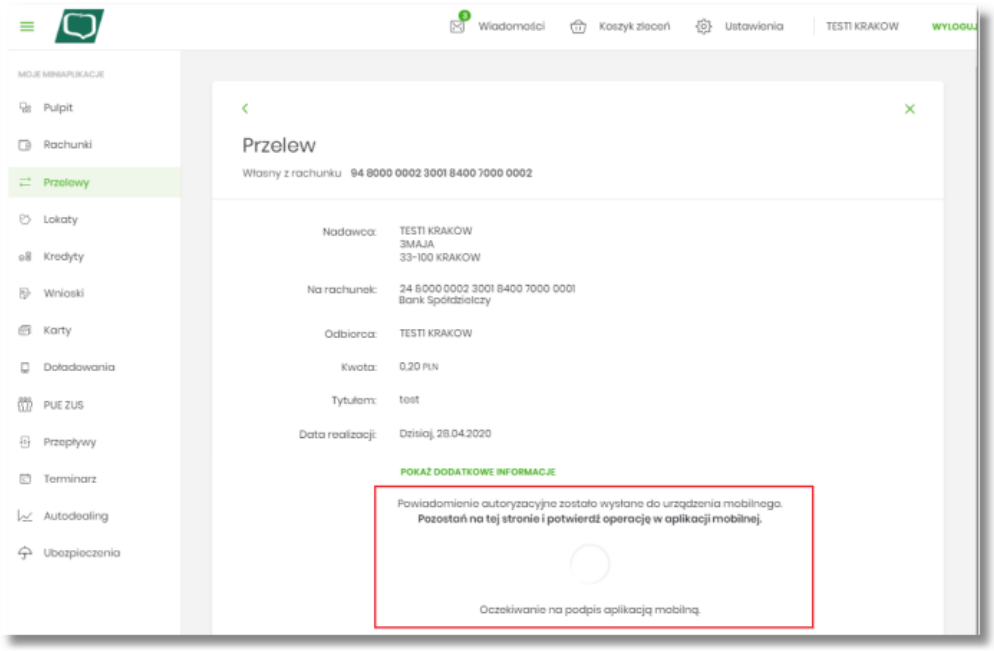
W przypadku autoryzacji zleceń złożonych w systemie Asseco CBP/EBP użytkownik otrzyma powiadomienie PUSH oraz dokona autoryzacji operacji w aplikacji mobilnej.

Proces autoryzacji dyspozycji przychodzącej z zewnątrz (system internetowy Asseco CBP/EBP), przed zalogowaniem użytkownika w aplikacji hybrydowej na urządzeniu mobilnym

1. Użytkownik składa dyspozycję w bankowości internetowej CBP/EBP i wybiera opcję autoryzacji dyspozycji

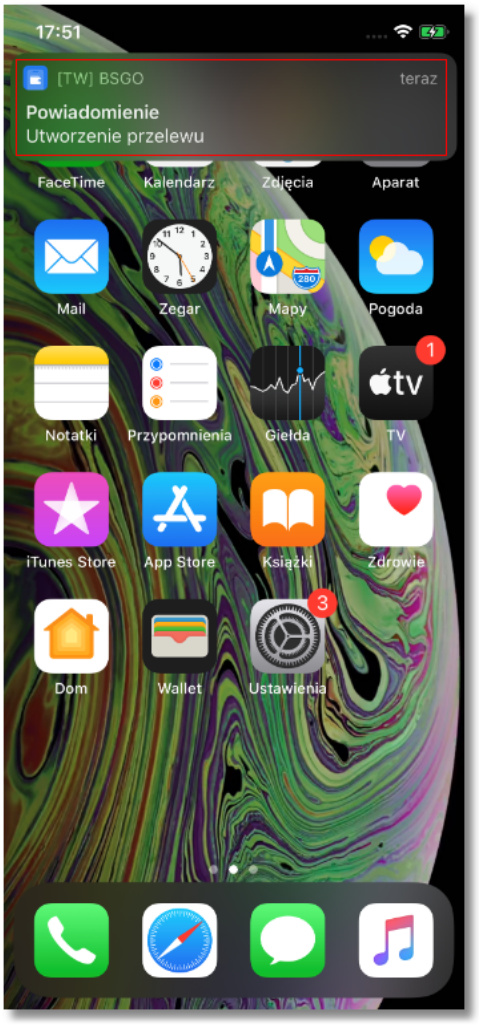


2. System bankowości internetowej CBP prezentuje ekran informujący o wysłaniu dyspozycji do autoryzacji na aplikację mobilną.

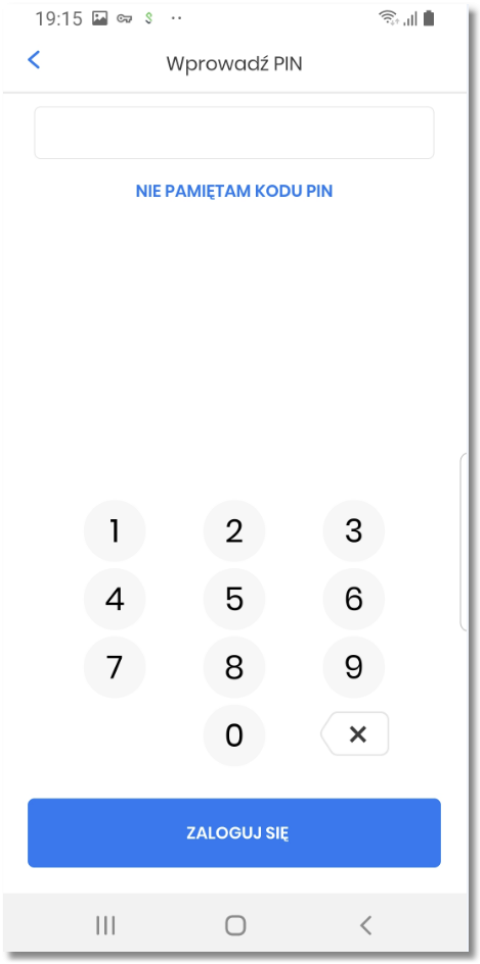


3. System bankowości internetowej CBP wysyła do aplikacji mobilnej powiadomienie PUSH o nowej dyspozycji do autoryzacji.

4. Aplikacja wyświetla na urządzeniu mobilnym baner powiadomienia PUSH z informacją o oczekującym zleceniu autoryzacyjnym.



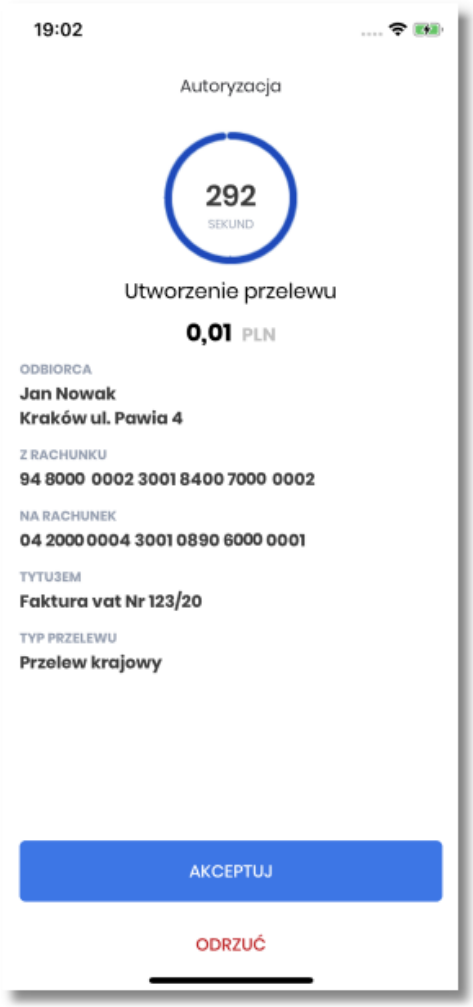
5. Użytkownik wybiera baner powiadomienia PUSH, które uruchamia aplikację hybrydową, wyświetlany jest ekran logowania do aplikacji **Wprowadź PIN**.



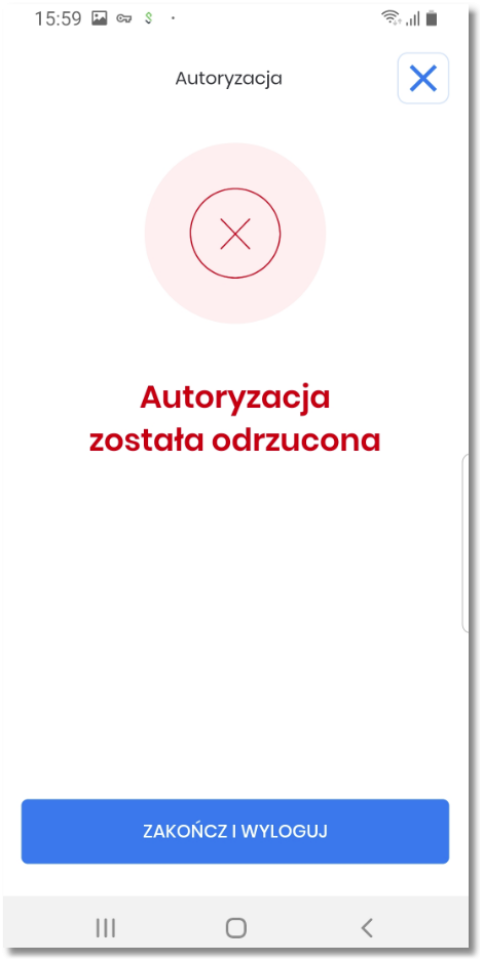
6. Użytkownik loguje się do aplikacji hybrydowej za pomocą kodu PIN lub danych biometrycznych zdefiniowanego przez użytkownika w procesie aktywacji aplikacji hybrydowej.

7. Aplikacja hybrydowa pobiera z systemu dane do autoryzacji.

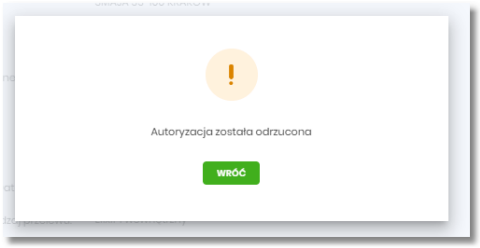
8. Aplikacja hybrydowa po zalogowaniu prezentuje dane dyspozycji do autoryzacji, w celu przejścia na ekran potwierdzenia operacji należy wybrać przycisk [AKCEPTUJ].



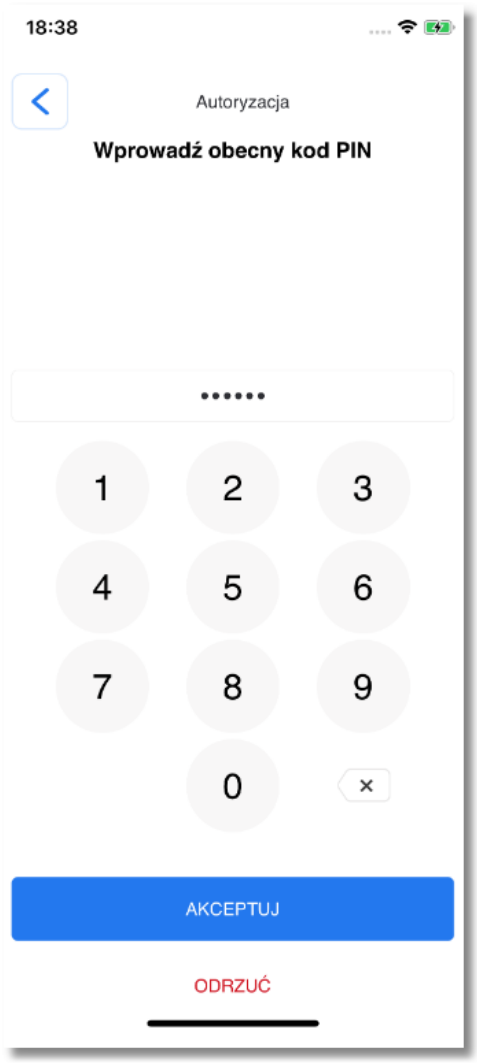
Wybór przycisku [ODRZUĆ] powoduje odrzucenie potwierdzenia autoryzacji i ustawienie statusu dyspozycji na odrzucona.



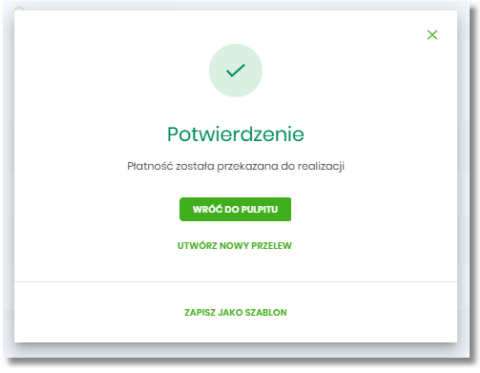
W systemie bankowości internetowej CBP/EBP prezentowany jest komunikat o odrzuceniu autoryzacji dyspozycji.



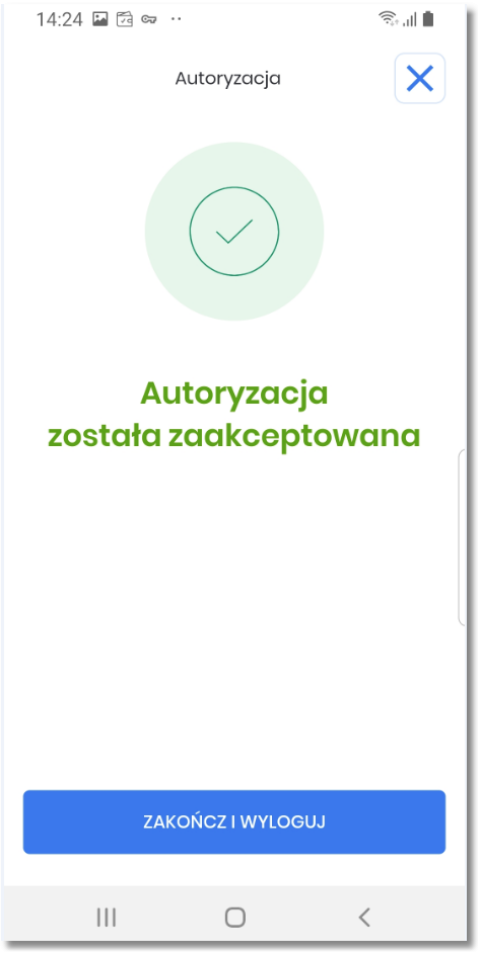
9. W przypadku podjęcia przez użytkownika decyzji o akceptacji dyspozycji, użytkownik weryfikuje wprowadzone dane oraz potwierdza realizację dyspozycji poprzez wprowadzenie poprawnego kodu PIN oraz wybór przycisku [AKCEPTUJ], na tym kroku użytkownik ma również możliwość odrzucenia dyspozycji.



10. Aplikacja hybrydowa podpisuje dyspozycję za pomocą klucza prywatnego.
11. Aplikacja hybrydowa wysyła podpisaną dyspozycję do systemu.
12. System weryfikuje podpis dyspozycji złożony w aplikacji hybrydowej, przekazuje wynik do aplikacji hybrydowej oraz do systemu bankowości internetowej CBP (weryfikacja pozytywna).
13. System bankowości internetowej CBP prezentuje potwierdzenie autoryzacji dyspozycji.

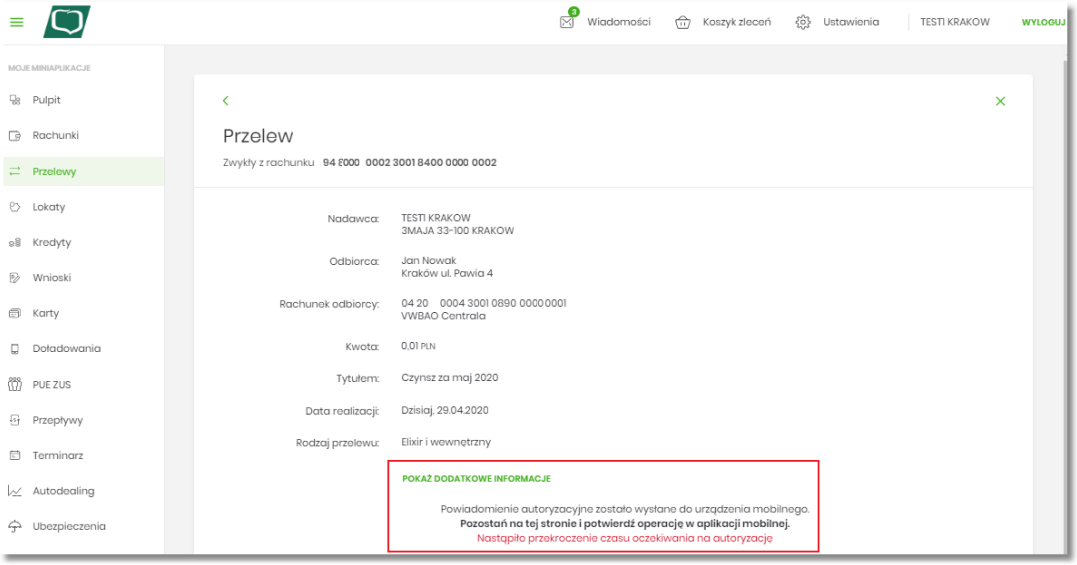


14. Aplikacja hybrydowa prezentuje potwierdzenie autoryzacji dyspozycji.



W przypadku, gdy użytkownik nie podpisał dyspozycji w określonym czasie po wskazaniu dyspozycji w aplikacji mobilnej Asseco MAA preznetowany jest komunikat informujący o błędnej akceptacji.

W systemie bankowości internetowej def3000/CBP na ekranie dyspozycji prezentowany jest komunikat informujący o przekroczeniu czasu oczekiwania na autoryzację.



W przypadku wprowadzenia błędnego kodu PIN na ekranie system prezentuje komunikat walidacyjny *"Wprowadzony PIN jest nieprawidłowy"*. Użytkownik ma możliwość ponownego wprowadzenia kodu PIN lub

wyjść z formatki autoryzacji nie podejmując żadnej decyzji (odrzucenia/akceptacji). Użytkownik może ponownie wybrać autoryzację z listy (o ile nie upłynął czas ważności autoryzacji), natomiast w def3000/CBP system czeka aż upłynie określony czas oczekiwania.

6.3. Autoryzacja dyspozycji zewnętrznej przychodzącej *po zalogowaniu*

Funkcjonalność **autoryzacji dyspozycji** złożonej w systemie internetowym Asseco CB/EBP, dla użytkownika **zalogowanego** do aplikacji hybrydowej przebiega tak samo jak dla użytkownika **nie zalogowanego** (opisanego powyżej) z ominięciem procesu logowania do aplikacji hybrydowej (kroki: 5,6).

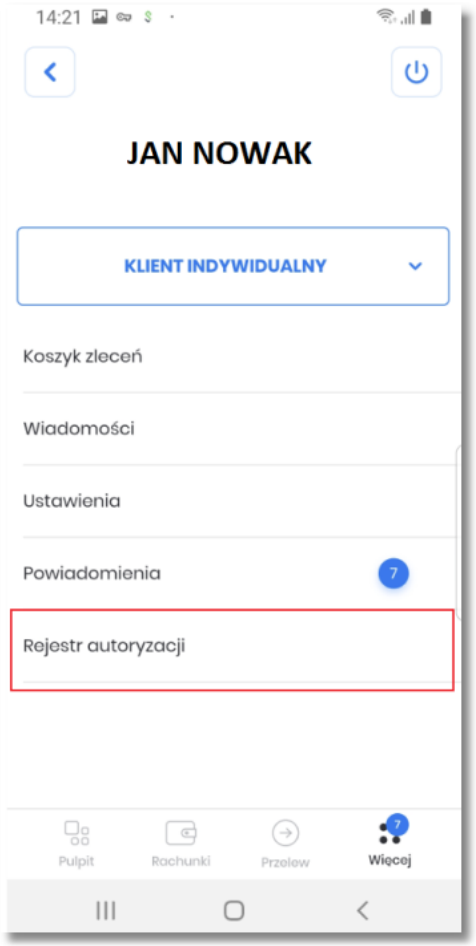
W przypadku wprowadzenia przez użytkownika **trzykrotnie błędnego PIN-u**, aplikacja zostaje **zablokowana**! Wyświetlany jest stosowny komunikat. Użytkownik musi ponownie dokonać aktywacji aplikacji w celu korzystania z niej.

7. Rejestr autoryzacji

Opcja **Rejestr autoryzacji** jest listą zawierającą wszystkie dyspozycje oczekujące oraz zrealizowane w procesie autoryzacji oraz autentykacji, pochodzące z systemu internetowego Asseco CBP/EBP. Funkcjonalność umożliwia autoryzację wybranej z listy dyspozycji oczekującej oraz podgląd szczegółów wszystkich dyspozycji znajdujących się na liście.

Autoryzacja zleceń w aplikacji mobilnej realizowana jest za pomocą ustawionego kodu PIN. Metody biometryczne wykorzystywane są tylko w procesie logowania.

Aby przejść do rejestru należy wybrać opcję *Więcej* w dolnym menu aplikacji, użytkownikowi wyświetlana jest strona z dodatkowymi funkcjonalnościami.



Po wybraniu opcji **Rejestr autoryzacji** prezentowana jest lista dyspozycji złożonych w systemie bankowości internetowej, dla których wymagana jest autoryzacja.

Lista prezentuje następujące informacje:

- graficzny status zlecenia,
- graficzny licznik odmierzający czas jaki pozostał do autoryzacji zlecenia,
- czas utworzenia zlecenia w formacie DD.MM.RRR,
- tytuł zlecenia.

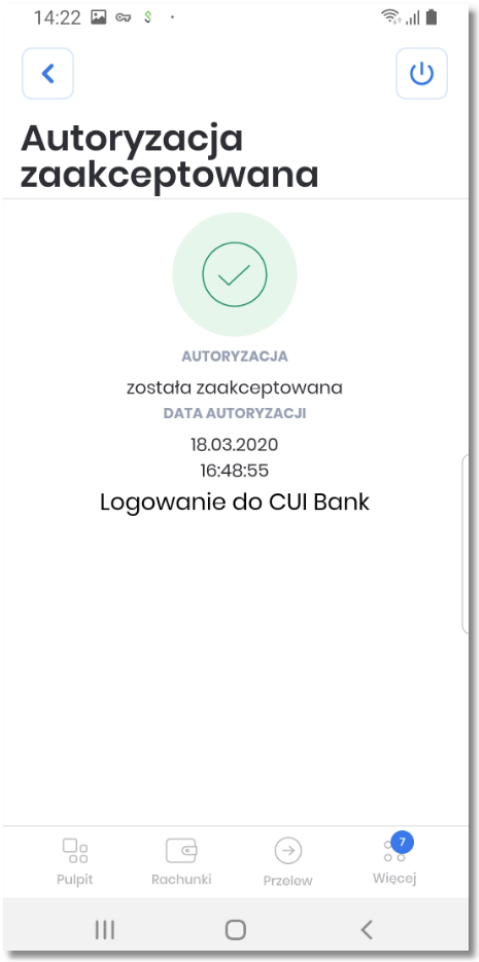
Dyspozycje, które zostały obsłużone lub czekają na podpis w aplikacji hybrydowej prezentowane są w następujących statusach:

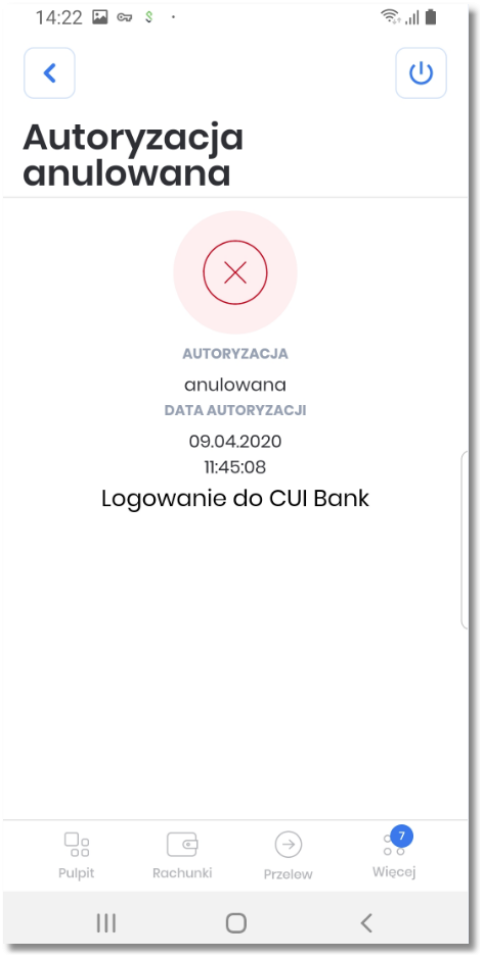
- ***Podpisana*** - użytkownik zaakceptował poprawnie dyspozycję, ikonka ,
- ***Anulowana*** - użytkownik nie zaakceptował dyspozycji w określonym czasie, ikonka ,
- ***Odrzucona*** - użytkownik odrzucił autoryzację dyspozycji, ikonka .
- ***Oczekująca*** - użytkownik posiada dyspozycję do akceptacji zdefiniowaną w systemie CBP oczekującą na autoryzację dyspozycji, ikonka oraz wyróżnieniem poprzez pogrubienie opisu.

Rejestr autoryzacji umożliwia:

- podgląd szczegółów zlecenia,
- autoryzację zlecenia oczekującego.

W pierwszym przypadku wybór pozycji na liście przenosi użytkownika do podglądu szczegółów autoryzowanej dyspozycji.





W drugim po wybraniu z listy dyspozycji oczekującej użytkownik ma możliwość autoryzacji jej kodem PIN, do momentu upłynięcia czasu, przeznaczonego na akceptację zlecenia. Dyspozycja oczekująca na autoryzację w systemie Asseco Hybryda prezentowane są na górze listy autoryzacji. W ramach obsługi autoryzacji dyspozycji w danym czasie może być dostępna wyłącznie jedna dyspozycja do autoryzacji. Dyspozycje mają określony czas ważności, po upływie którego są anulowane - autoryzacja nie jest możliwa. Dyspozycja zostaje odrzucona.

W górnej części formularza **Rejestr autoryzacji** dostępne są przyciski:

- – umożliwiający cofnięcie się do wcześniej wyświetlanego użytkownikowi ekranu
- – umożliwiający wylogowanie z aplikacji.

Autoryzacja dyspozycji w aplikacji realizowana jest poprzez moduł Asseco MAA, który stanowi integralną część hybrydowej aplikacji mobilnej.

W przypadku transakcji wymagającej autoryzacji złożonej w systemie Asseco CBP/EBP użytkownik otrzyma powiadomienie PUSH i uzyska możliwość autoryzacji operację w aplikacji mobilnej.

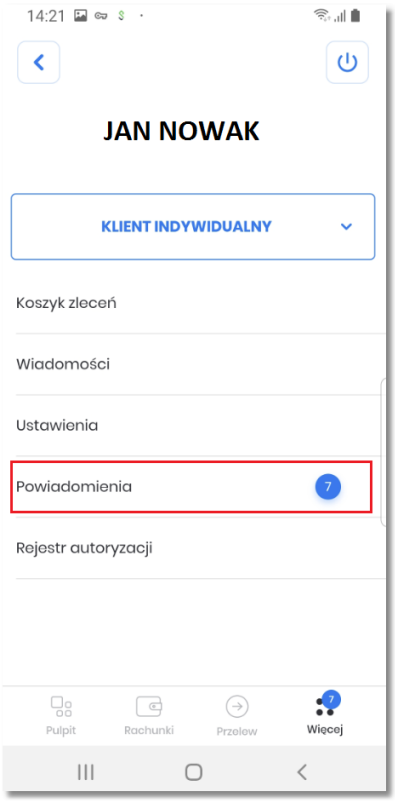
8. Powiadomienia

Funkcjonalność **Powiadomienia** udostępnia użytkownikowi:

- szybką informację w postaci powiadomień PUSH
- listę powiadomień wraz z:
  - wyświetleniem szczegółów powiadomienia wraz z możliwością usnięcia
  - zbiorczym usuwaniem powiadomień
  - zbiorczym odczytywaniem powiadomień

Aby przejść do listy powiadomień, należy po zalogowaniu wybrać w *dolnym menu* pozycję 

[Więcej] a następnie wybrać [Powiadomienia].



System prezentuje ***licznik*** przy ikonie dolnego menu *Więcej* którego wartość jest sumą nowych wiadomości, powiadomień oraz zleceń w koszyku. Natomiast licznik znajdujący się przy funkcjonalności [POWIADOMIENIA] informuje o ilości nowych powiadomień na liście. Po usunięciu lub odczytaniu powiadomienia licznik zostaje automatycznie odświeżony.

8.1. Powiadomienia PUSH

Powiadomienia dotyczą informacji związanych z:

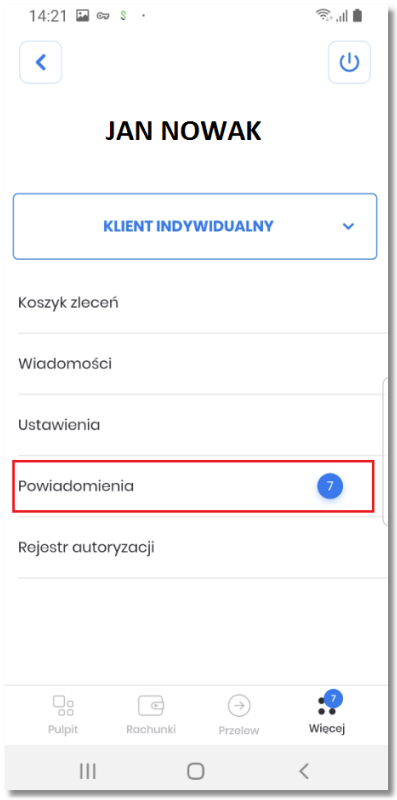
- powiadomieniami informacyjnymi (definiowane w systemie BO na poziomie klienta detalicznego oraz użytkownika np. wykonanie przelewu powyżej kwoty granicznej),
- powiadomieniami o logowaniu w kontekście danego użytkownika do aplikacji Asseco CBP/EBP,
- powiadomieniami autoryzacyjnymi nowych zleceń definiowanych w systemie Asseco CBP/EBP.

Powiadomienia PUSH, wyświetlane są zarówno gdy użytkownik jest zalogowany i korzysta z aplikacji hybrydowej jak i w momencie nie korzystania z systemu. Po wyświetleniu komunikatu PUSH ,użytkownik automatycznie zostaje przekierowany do strony logowania do aplikacji hybrydowej. W przypadku gdy użytkownik jest zalogowany i system otrzymuje informacje o nowych zleceniach do autoryzacji w systemie CBP/EBP, wówczas wyświetlane są one automatycznie na pierwszym ekranie aplikacji.

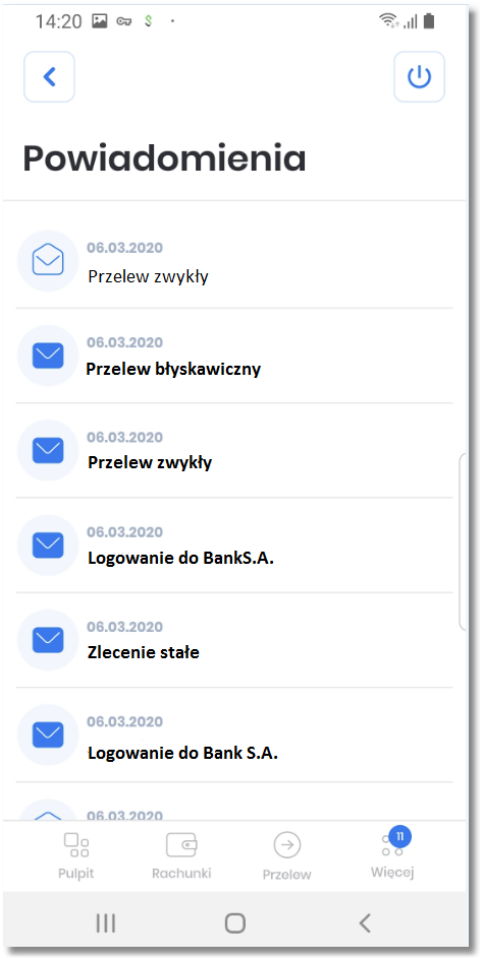
8.2. Lista powiadomień

Aby przejść do **Listy powiadomień**, należy po zalogowaniu wybrać w *dolnym menu* pozycję 

[Więcej] a następnie wybrać [Powiadomienia].



Użytkownikowi wyświetlana jest lista powiadomień.



Lista wyświetla powiadomienia przychodzące w kolejności chronologicznej. Dla każdego powiadomienia na liście wyświetlane są następujące informacje:

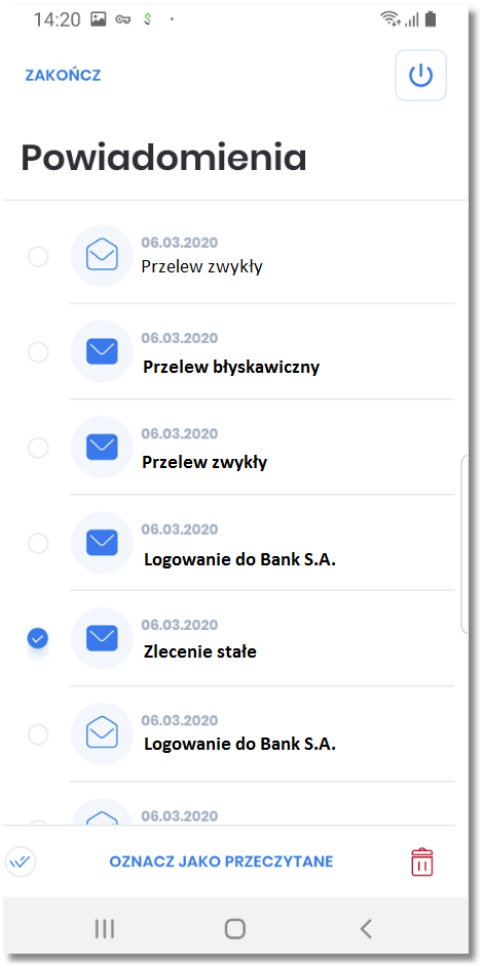
- **data** - data utworzenia powiadomienia w formacie DD.MM.RRRR
- **tytuł** - tytuł powiadomienia, wyróżniony pogrubieniem dla powiadomień nieodczytanych
- **status powiadomienia** w postaci znaku graficznego:
  - - powiadomienie odczytane
  - - powiadomienie nieodczytane

Wybór pozycji na liście powiadomień przenosi użytkownika do podglądu [SZCZEGÓŁÓW POWIADOMIENIA] zawierających:

- podstawowe informacje wyświetlane na liście: status, tytuł oraz datę utworzenia powiadomienia
- dodatkowe szczegółowe informacje dotyczące wybranego powiadomienia,
- USUŃ POWIADOMIENIE - akcję umożliwiającą automatyczne usunięcie powiadomienia.

Użytkownik ma możliwość zarządzania listą poprzez **zbiorcze zarządzanie usuwaniem i odczytywaniem powiadomień**, w tym celu w wybranym wierszu listy należy kliknąć podwójnie w wiersz (tzw. dwuklik).

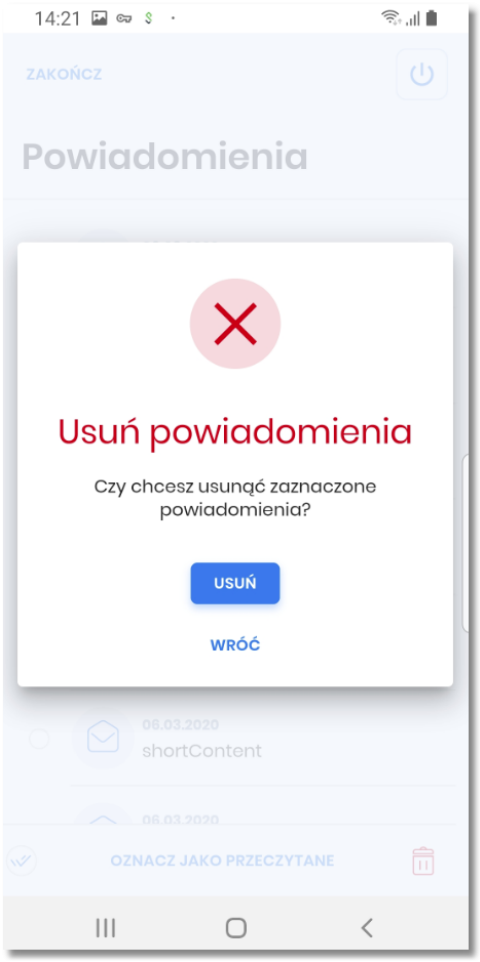
Użytkownik przechodzi w tryb edycji listy.

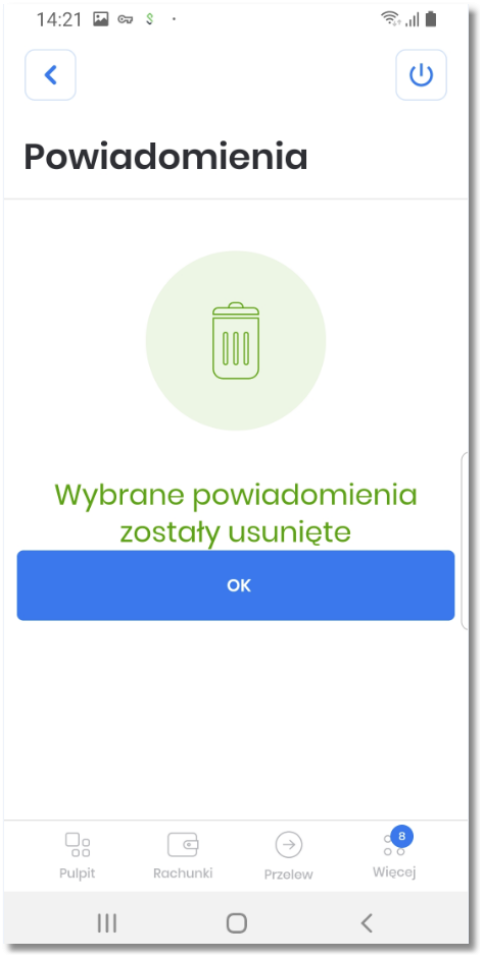


Formularz **Powiadomienia** w trybie edycji prezentuje:

- przy każdym powiadomieniu checkbox z możliwością - zaznaczenia - odznaczenia wybranych powiadomień
- dodatkowe dolne menu OZNACZ JAKO PRZECZYTANE z akcjami:
  - - umożliwia zaznaczenie/ odznaczenie wszystkich powiadomień widocznych na stronie,
  - OZNACZ JAKO PRZECZYTANE - umożliwia zbiorczą zmianę statusu na powiadomienia odczytane (wszystkie lub wybrane powiadomienia),
  - - umożliwia zbiorcze usunięcie powiadomień z listy (wszystkie lub wybrane powiadomienia),
- dodatkową akcję [ZAKOŃCZ] w górnym menu, umożliwiającą zakończenie edycji listy powiadomień.

System przed usunięciem powiadomienia wyświetla odpowiedni komunikat, po zaakceptowaniu którego dane powiadomienia zostają usunięte a użytkownik zostaje poinformowany o tym fakcie.


14:21
ZAKOŃCZ
Powiadomienia
Usuń powiadomienia
Czy chcesz usunąć zaznaczone powiadomienia?
USUŃ
WRÓĆ
06.03.2020
shortContent
OZNACZ JAKO PRZECZYTANE



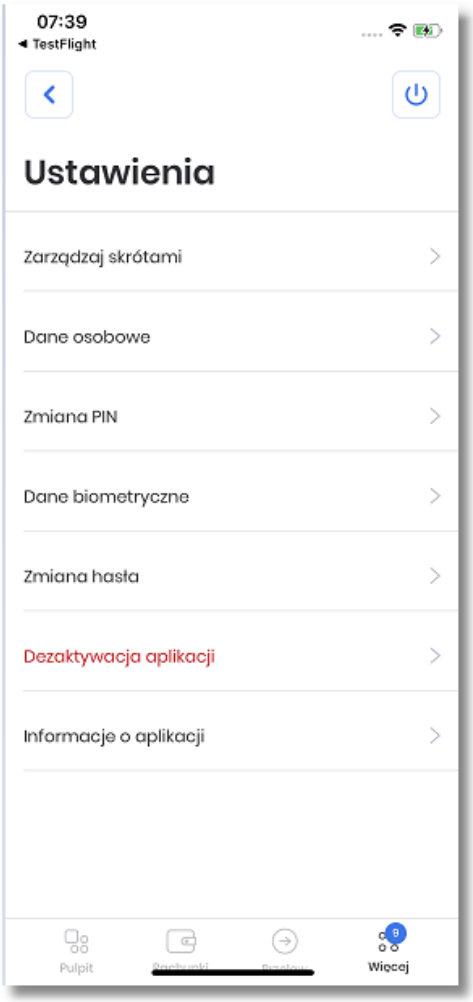
W górnej części formularza POWIADOMIENIA dostępne są przyciski:

- – umożliwiający przejście do poprzedniego ekranu prezentującego menu *Więcej*,
- – umożliwiający wylogowanie z aplikacji.

9. Ustawienia

Po zalogowaniu się do aplikacji i wybraniu w ***dolnym menu*** pozycji **Więcej**, użytkownikowi wyświetlana jest strona z dodatkowymi funkcjonalonościami. Po wybraniu akcji **Ustawienia** użytkownikowi wyświetlona jest lista opcji:

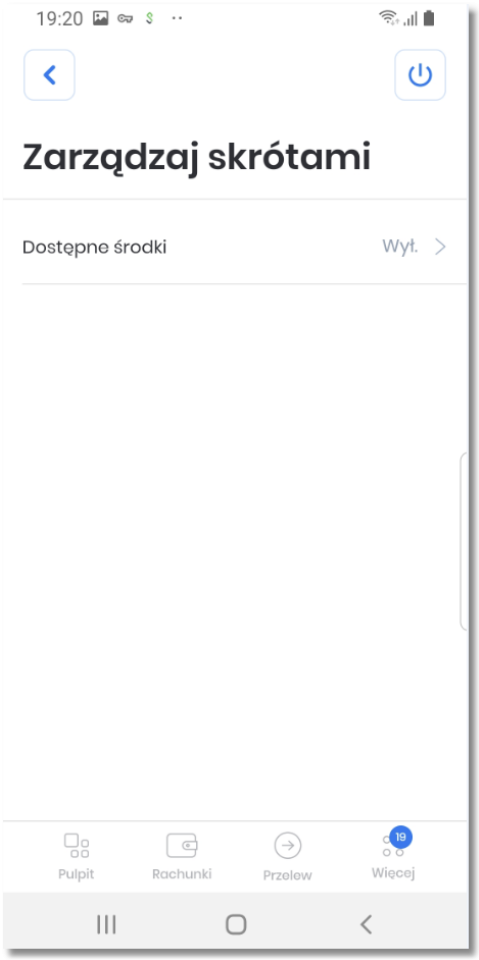
- **Zarządzanie skrótami** - formatka z możliwością włączenia/wyłączenia prezentacji dostępnych środków na ekranie początkowym aplikacji Asseco Hybryda,
- **Dane osobowe** - formatka z możliwością podglądu danych użytkownika aplikacji Asseco Hybryda,
- **Zmiana PIN** - formatka z możliwością zmiany pinu w aplikacji Asseco Hybryda,
- **Dane biometryczne** - formatka z możliwością włączenia/wyłączenia logowania się przy użyciu danych biometrycznych do aplikacji Asseco Hybryda,
- **Dezaktywacja aplikacji** - możliwość dezaktywacji aplikacji Asseco Hybryda,
- **Informacje o aplikacji** - prezentacja informacji o aplikacji Asseco Hybryda.



9.1. Zarządzanie skrótami

Opcja **Zarządzanie skrótami** umożliwia użytkownikowi włączenie/wyłączenie prezentacji informacji o saldzie (dostępnych środkach) na wybranym rachunku, na ekranie początkowym aplikacji Asseco Hybryda.

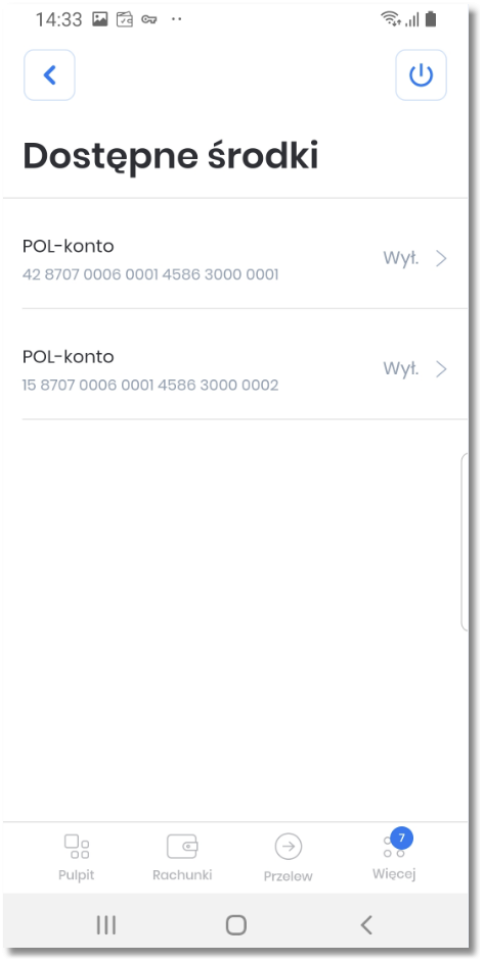
W pierwszym kroku należy wybrać opcje [Dostępne środki] Włącz/Wyłącz, pozwalająca na uruchomienie zarządzania skrótem.



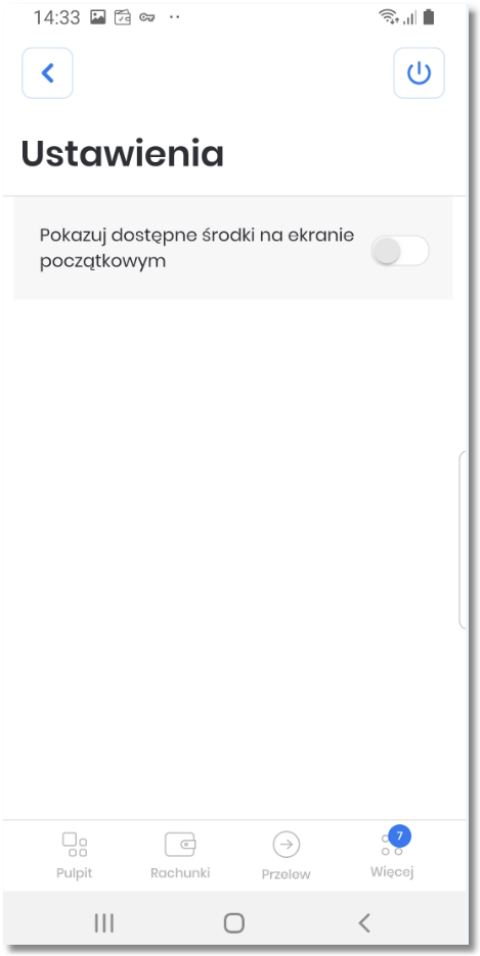
Po zatwierdzeniu użytkownikowi wyświetlana jest lista jego rachunków, dla których możliwe jest ustawienie wyświetlania salda na ekranie powitalnym.

Na liście prezentowane są:

- nazwa rachunku
- numer rachunku
- informacja o prezentacji dostępnych środków dla rachunku Wł.(włączona)/ Wył.(wyłączona)

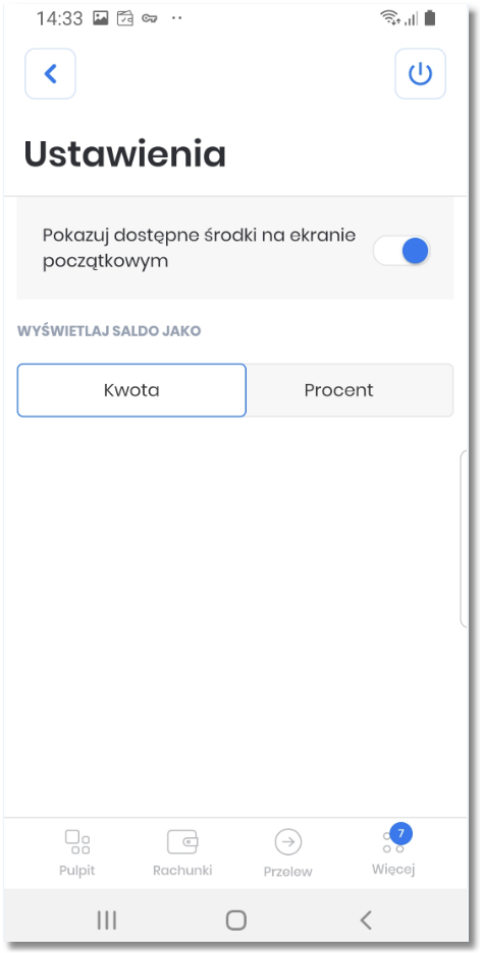


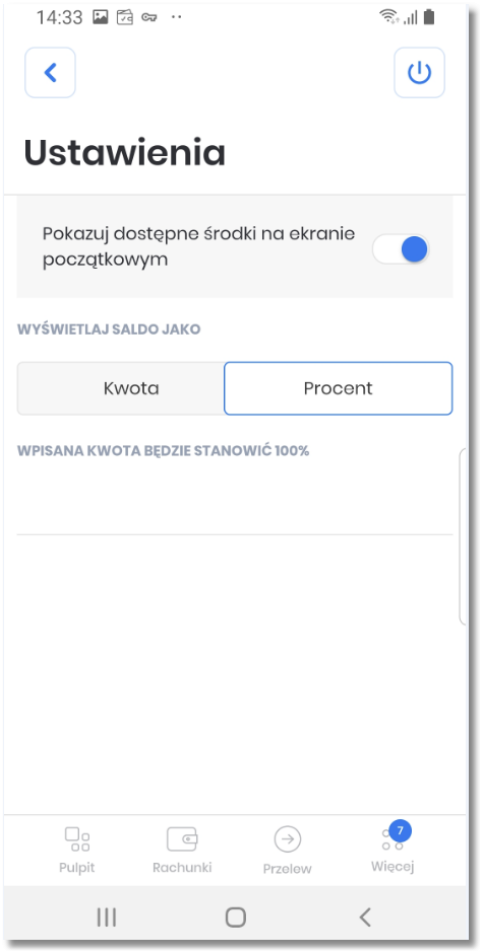
Następnie poprzez kliknięcie w wybrany rachunek użytkownik przechodzi do kolejnego kroku, na którym włącza/ wyłącza skrót dla konkretnego rachunku poprzez zaznaczenie opcji [Pokazuj dostępne środki na ekranie początkowym].

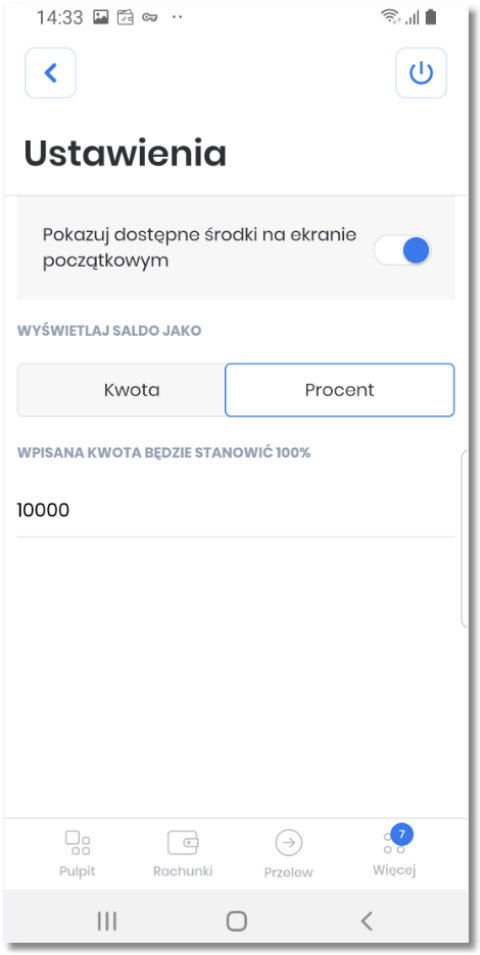


Po zatwierdzeniu użytkownikowi prezentowane jest kolejne ustawienie dotyczące formy prezentacji, możliwe opcje to:

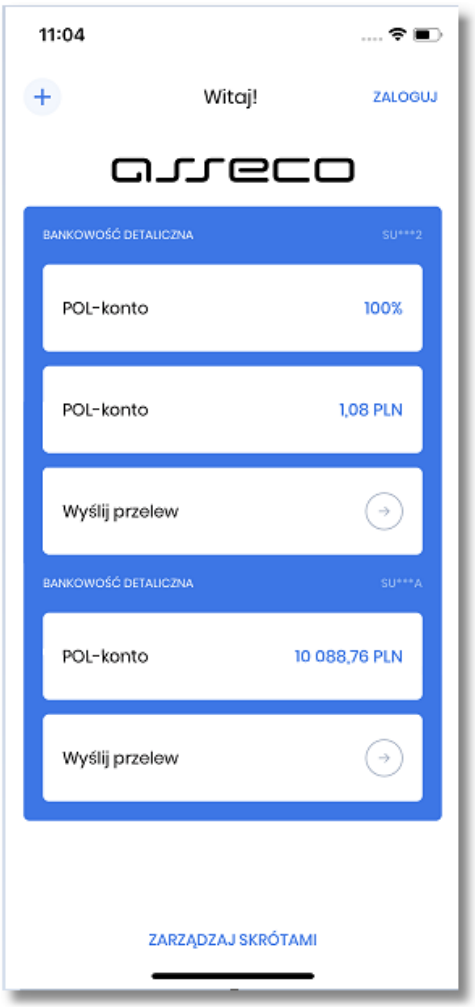
- wyświetlenie salda jako kwoty w PLN,
- prezentacja procentowa dostępnych środków na koncie, dla której możemy dodatkowo zdefiniować kwotę stanowiącą 100 %.


14:33
Ustawienia
Pokazuj dostępne środki na ekranie początkowym
WYŚWIETLAJ SALDO JAKO
Kwota
Procent
Pulpit
Rachunki
Przelew
Więcej


14:33
Ustawienia
Pokazuj dostępne środki na ekranie początkowym
WYŚWIETLAJ SALDO JAKO
Kwota
Procent
WPISANA KWOTA BĘDZIE STANOWIĆ 100%
Pulpit
Rachunki
Przelew
Więcej



Po dokonaniu ustawień na ekranie początkowym zostaną zaprezentowane ustawione dane.



Funkcjonalność ***Zarządzania skrótami*** dostępna jest tylko dla kontekstu domyślnego (ustawionego po zalogowaniu). W przypadku wyboru innego kontekst niż domyślny (dolne menu 'Więcej') opcja ta jest niedostępna.

9.2. Dane osobowe

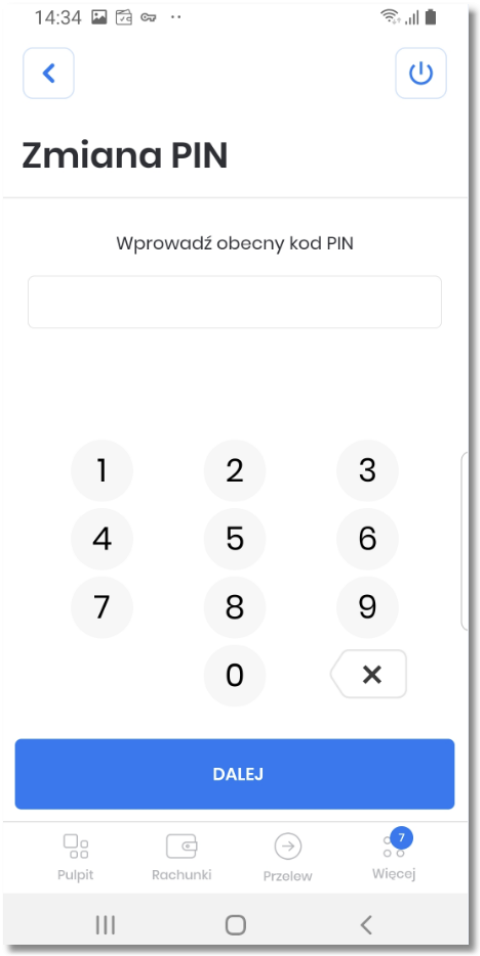
Opcja **Dane osobowe** prezentuje podstawowe informacje o użytkowniku takie jak:

- imię i nazwisko,
- PESEL,
- NIP,
- numer dowodu osobistego,
- data wystawienia dowodu osobistego,
- wystawca dowodu osobistego,
- adres zamieszkania,

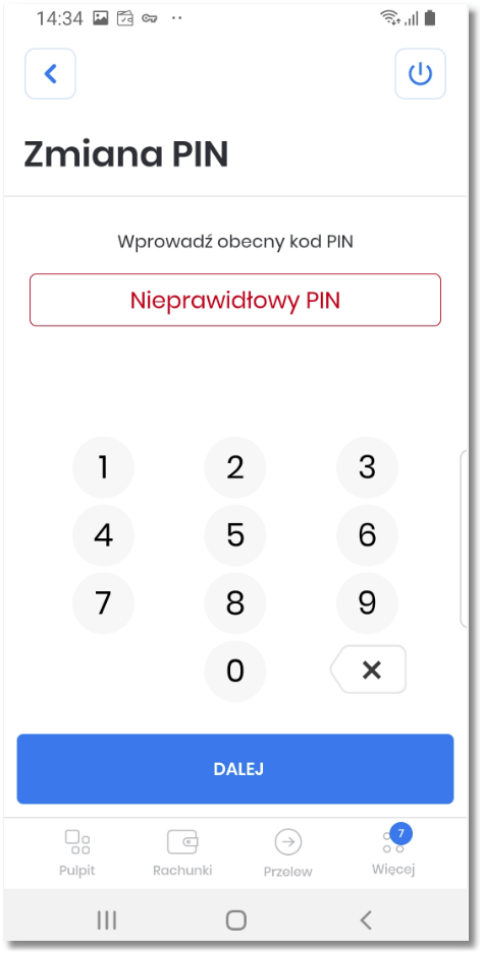
- adres do korespondencji,
- adres e-mail,
- numer telefonu do kontaktu.

9.3. Zmiana PIN

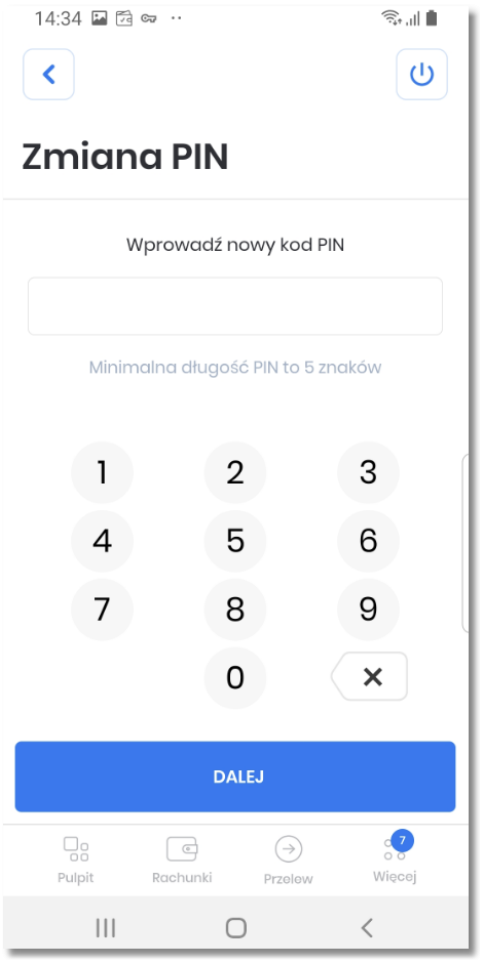
Opcja **Zmiana PIN** umożliwia użytkownikowi zmianę obecnego kodu PIN do aplikacji Asseco Hybryda na nowy. W pierwszym kroku należy wpisać obecny PIN i potwierdzić przyciskiem [DALEJ] przechodząc do kolejnego kroku.



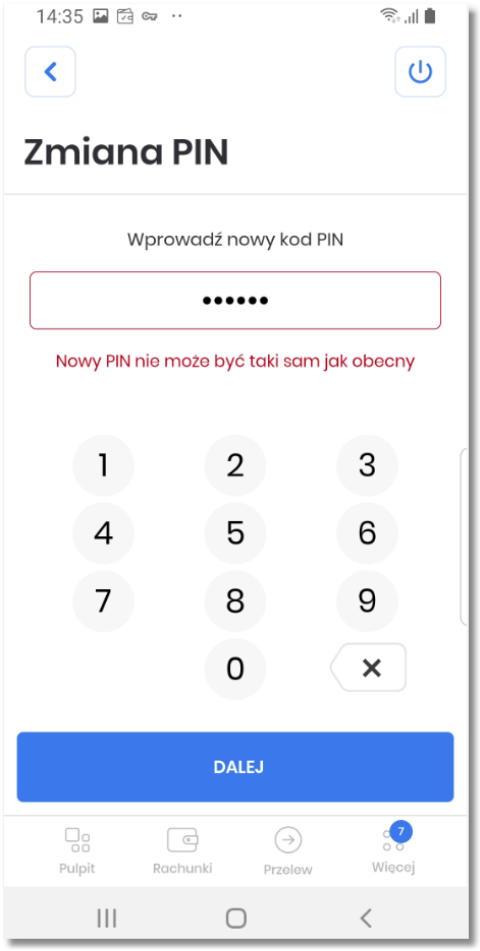
System sprawdza poprawność obecnego PIN-u i w przypadku niezgodności wyświetla odpowiedni komunikat.



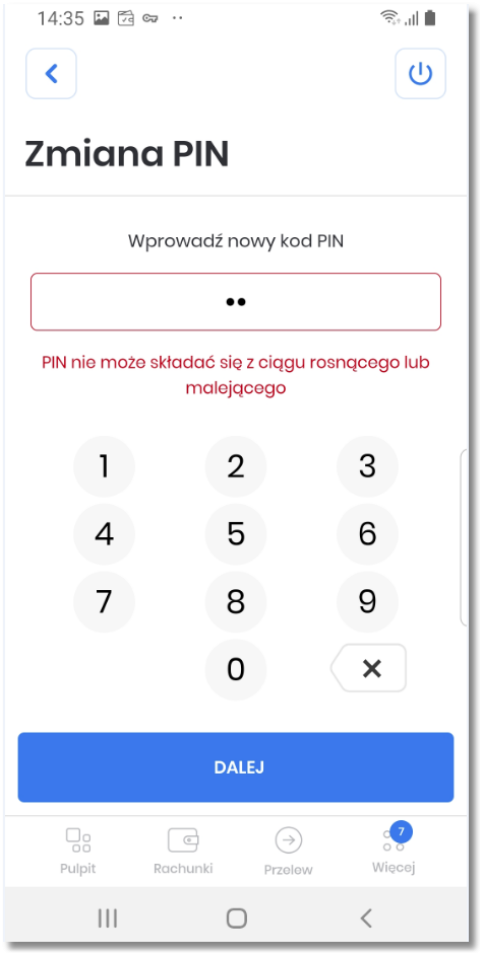
Na kolejnym kroku użytkownik wprowadza nowy PIN, którym chce się logować i wybór zatwierdza przyciskiem [DALEJ], przechodząc do kolejnego kroku.

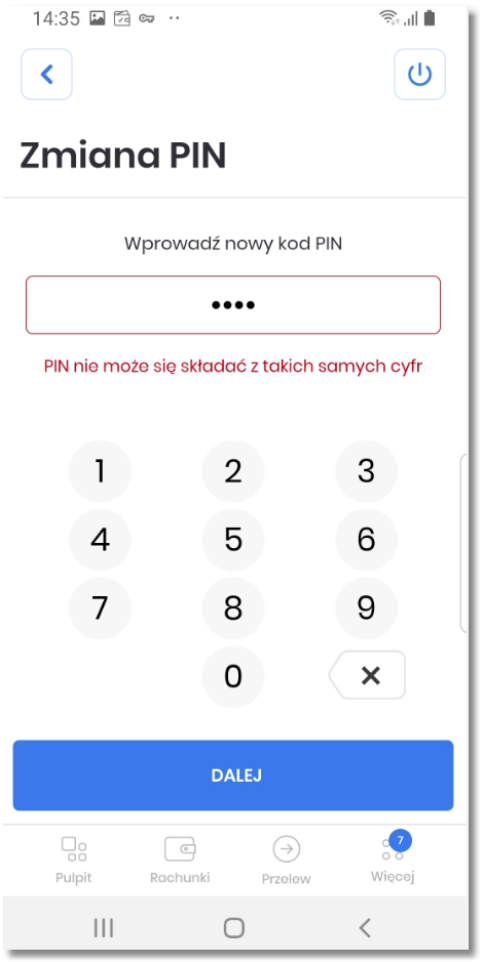


System weryfikuje poprawność obecnego PIN-u z nowym i w przypadku niezgodności wyświetlany jest odpowiedni komunikat.

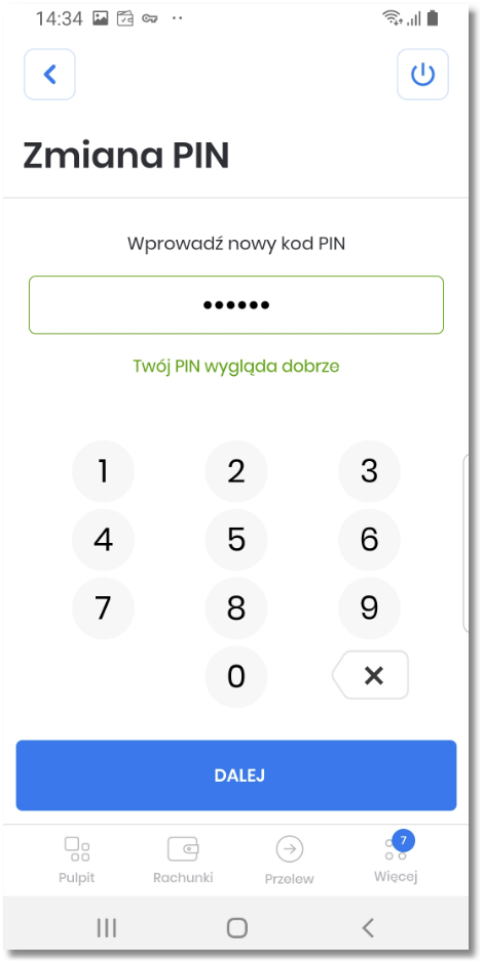


System weryfikuje poprawność obecnego PIN-u pod kątem wprowadzania prostych haseł takich jak 11111, 22222, 123123, 12345. W przypadku zdefiniowania takiej kombinacji cyfr w systemie zostanie zaprezentowany stosowny komunikat walidacyjny.

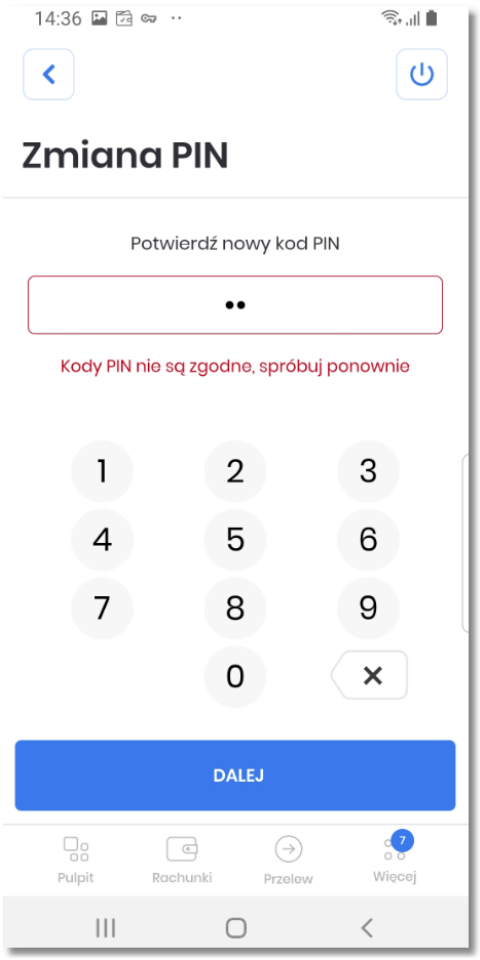

14:35
Zmiana PIN
Wprowadź nowy kod PIN
PIN nie może składać się z ciągu rosnącego lub malejącego
1
2
3
4
5
6
7
8
9
0
DALEJ
Pulpit
Rachunki
Przelew
Więcej



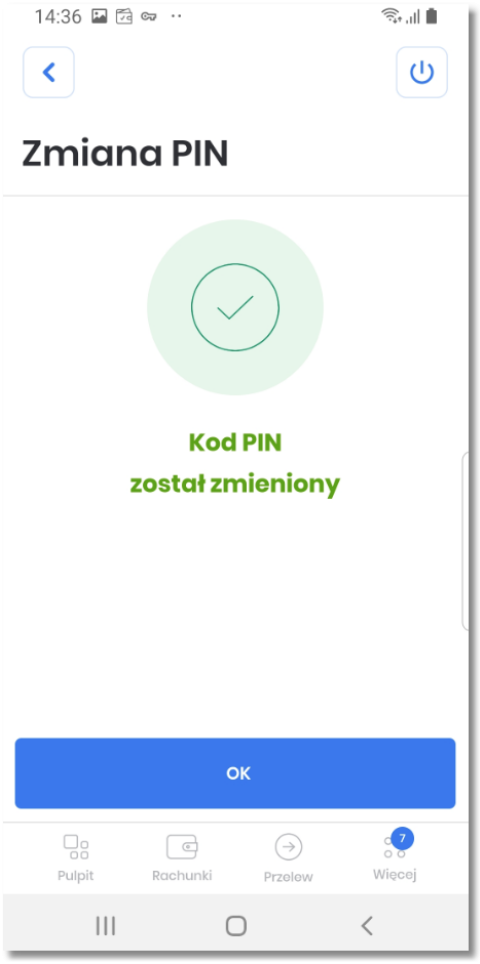
Dla prawidłowej weryfiakcji nowego PIN-u, wyświetlany jest komuniat.



Następnie użytkownik potwierdza wpisany PIN, który jest automatycznie sprawdzany co do zgodności z nowym PIN-em.



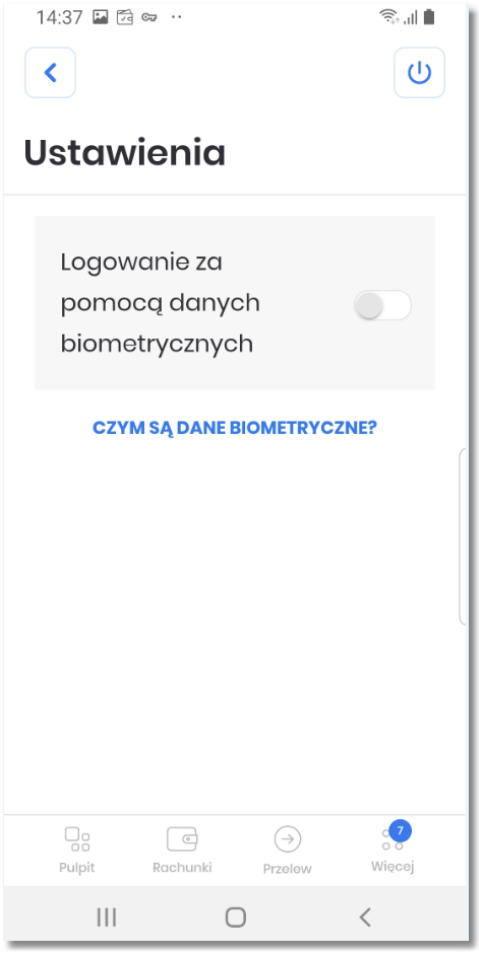
Po poprawnej zmianie kodu PIN i zatwierdzeniu przyciskiem [DALEJ], system informuje o zakończeniu procesu zmiany PIN-u.



W przypadku, gdy użytkownik w polu Wprowadź obecny PIN wprowadzi błędny aktualny kod PIN a następnie zatwierdzi przyciskiem [DALEJ], system poinformuje o odrzuceniu operacji. Po podaniu 3 błędnych kodów PIN aplikacja zostanie zablokowana automatycznie.

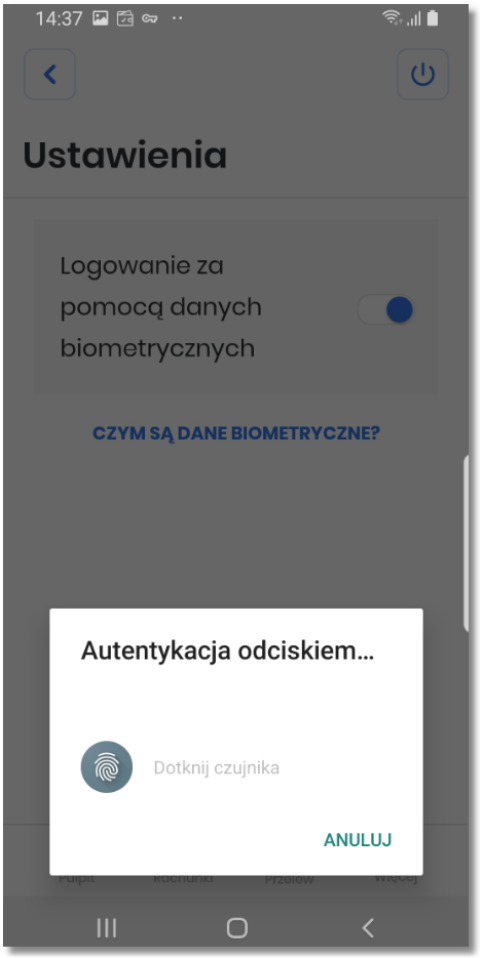
9.4. Dane biometryczne

Opcja ***Dane biometryczne*** umożliwia włączenia/wyłączenia logowania się przy użyciu danych biometrycznych do aplikacji Asseco Hybryda dla urządzeń mobilnych posiadających włączoną taką opcję.

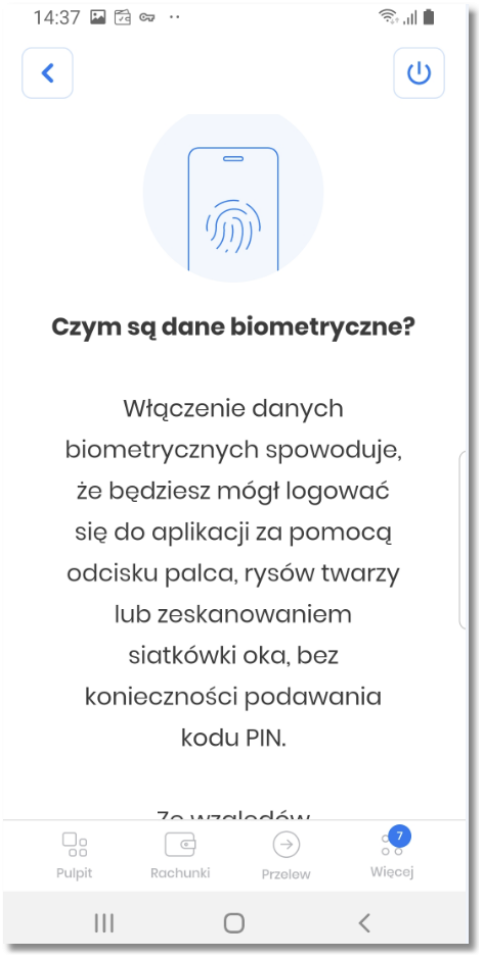


Dla urządzeń mobilnych z wyłączonym inteligentnym skanowaniem, opcja ta jest ukryta.

Włączenie danych biometrycznych umożliwia logowanie się do aplikacji za pomocą odcisku palca, rysów twarzy bez konieczności podawania kodu PIN.



Na stronie znajduje się link **CZYM SĄ DANE BIOMETRYCZNE**, po wybraniu którego, użytkownikowi wyświetlane są informacje.

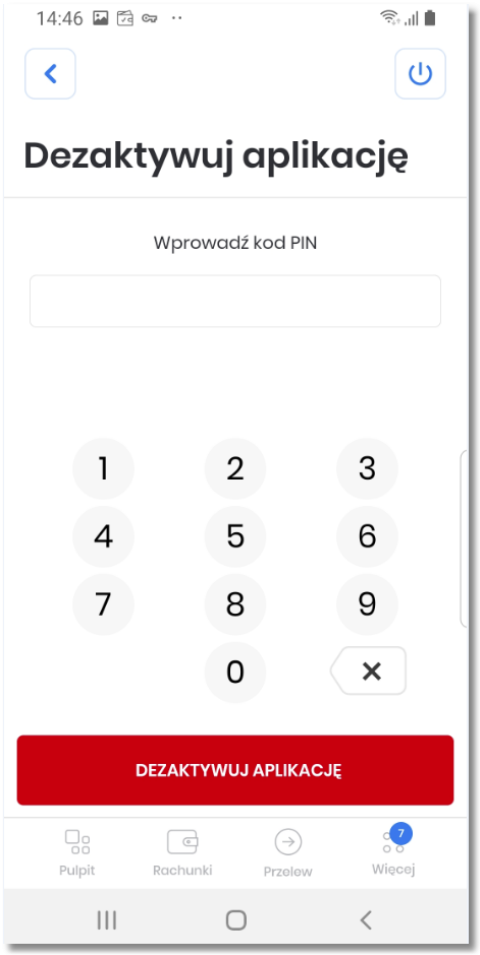


Dodatkowe informacje opisane są w rozdziale *Logowanie przy użyciu metody biometrycznej*.

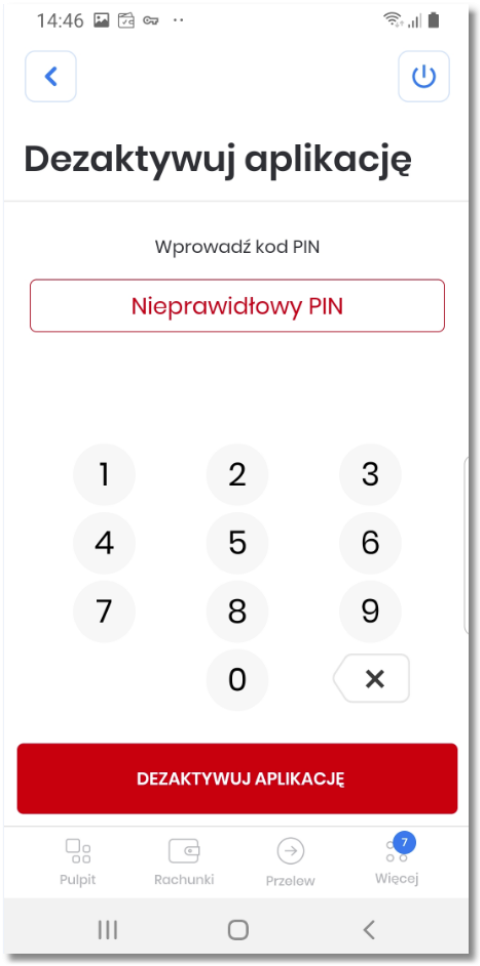
9.5. Dezaktywacja aplikacji

Opcja ***Dezaktywacja aplikacji*** umożliwia dezaktywację aplikacji Asseco Hybryda, która skutkuje blokadą możliwości wykonania autoryzacji. W tym celu należy kliknąć w przycisk [DEZAKTYWUJ APLIKACJĘ].

Następnie należy dokonać autoryzacji.



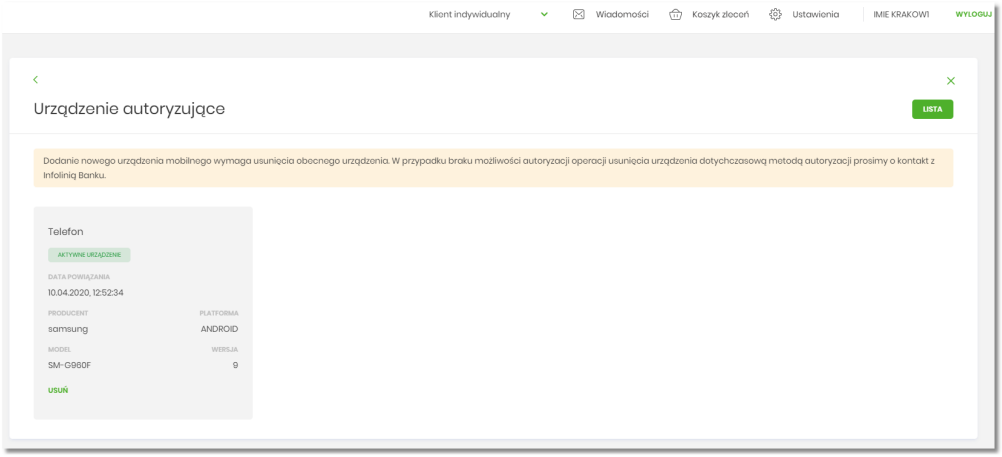
System weryfikuje poprawność wprowadzonych danych



Po prawidłowej weryfikacji PIN-u, użytkownikowi zostaje wyświetlony komunikat potwierdzający dezaktywację urządzenia.

Dodatkowo użytkownik może dezaktywować aplikację także:

- w Bankowości Internetowej, poprzez zalogowanie i usunięcie urządzenia autoryzującego, menu *Ustawienia* → *Urządzenie autoryzujące* → [USUŃ],

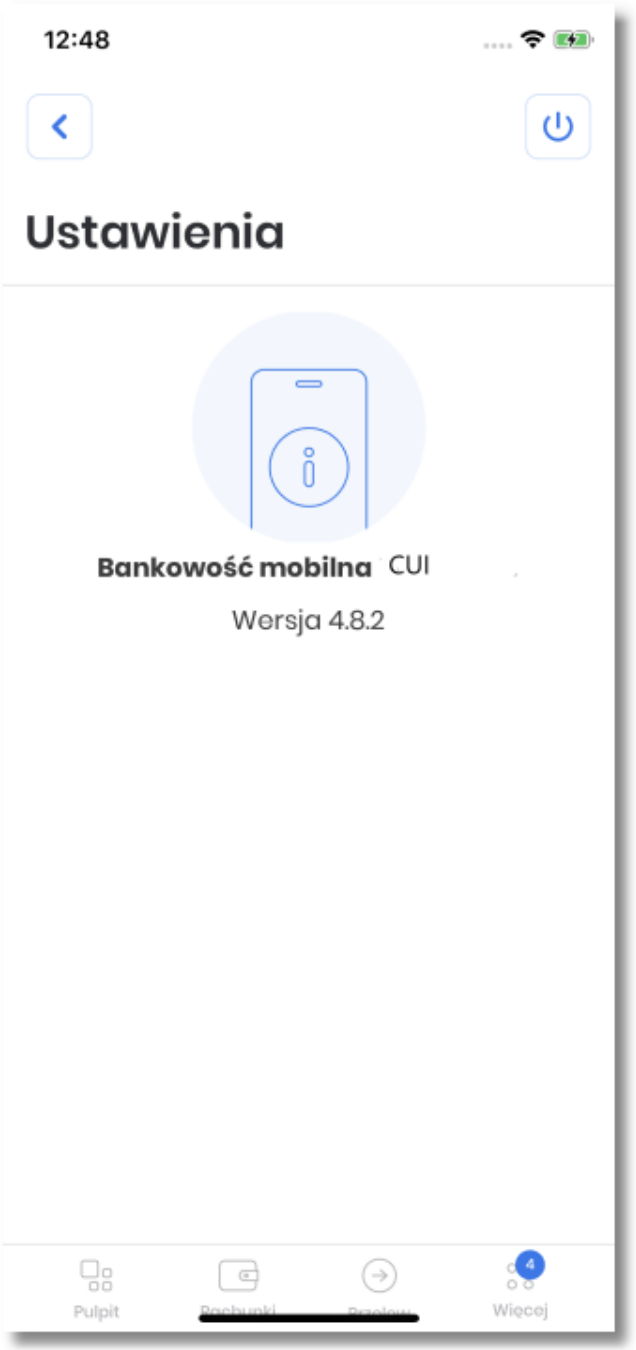


- poprzez kontakt z wybranym Call Center.

Ponowne użycie urządzenia wymaga także ponownej aktywacji aplikacji.

9.6. Informacje o aplikacji

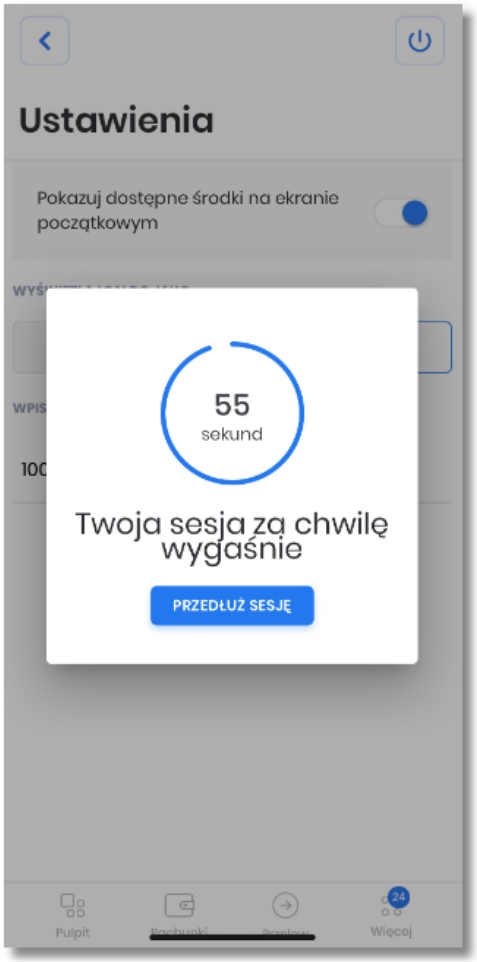
Opcja Informacje o aplikacji prezentuje informacje szczegółowe o aplikacji Asseco Hybryda, zawierające Nazwę aplikacji oraz jej wersję.



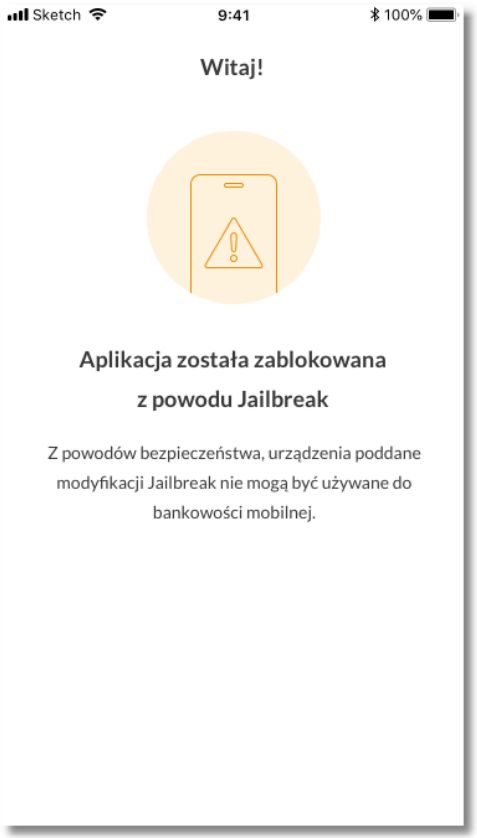
10. Wylogowanie

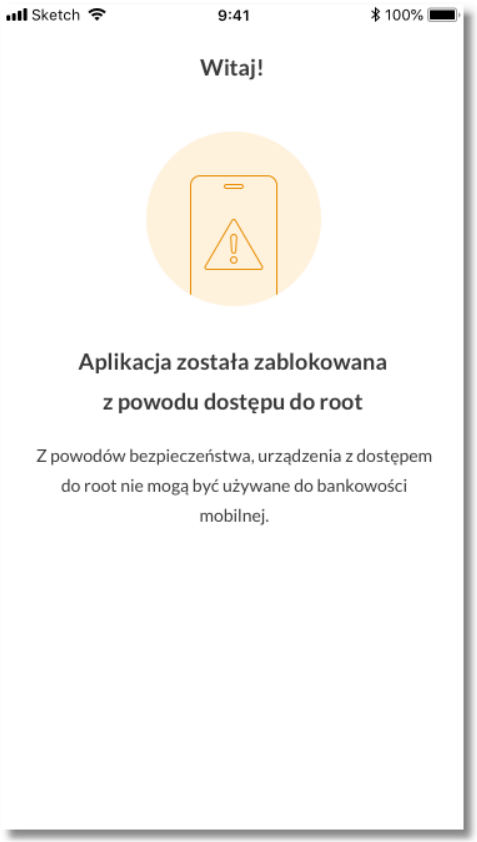
Zalogowany użytkownik po wybraniu ikony  znajdującej się w *górnym menu*, zostaje wylogowany z systemu. Wylogowanemu użytkownikowi automatycznie wyświetlana jest strona logowania do aplikacji, aby ponownie korzystać z aplikacji, wymagane jest ponowne zalogowanie.

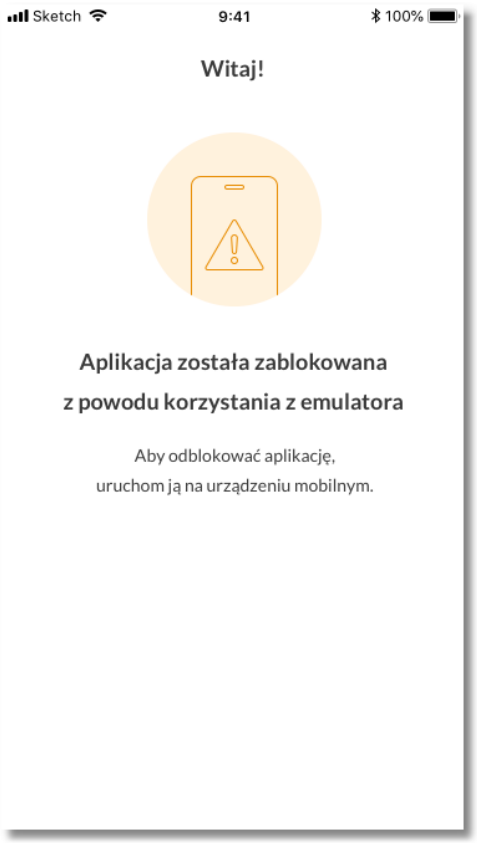
Aplikacja dokonuje także automatycznego wylogowania użytkownika, które następuje po upływie określonego czasu bezczynności użytkownika. Po automatycznym wylogowaniu i przywróceniu aplikacji użytkownik musi się ponownie zalogować.



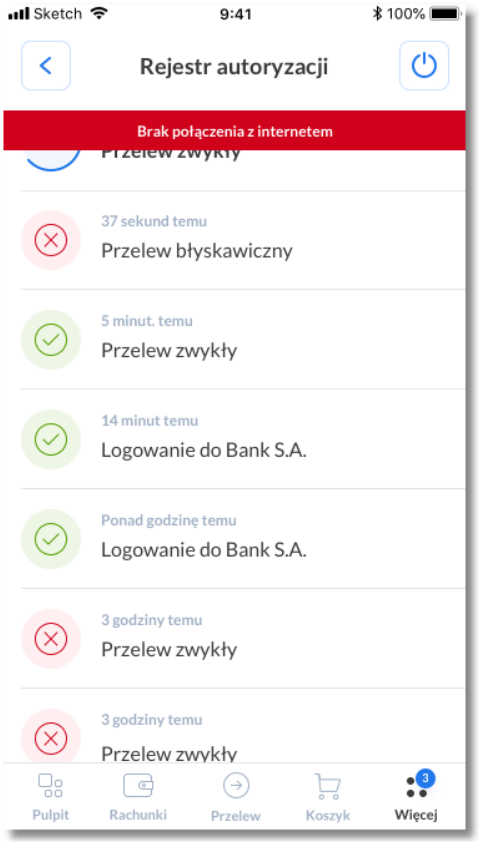
Dodatkowo aplikacja wykrywa i blokuje możliwości zalogowania się do aplikacji z powodów bezpieczeństwa. Użytkownikowi wyświetlane są następujące informacje:

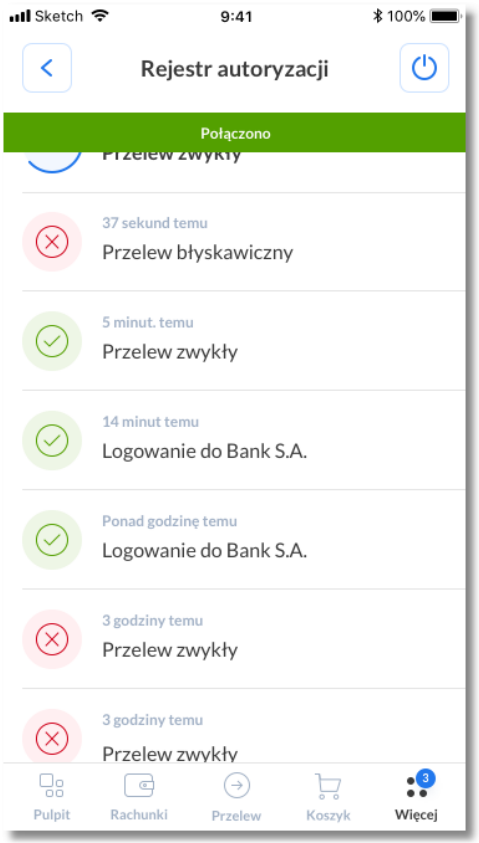

Sketch
9:41
100%
Witaj!
Aplikacja została zablokowana
z powodu Jailbreak
Z powodów bezpieczeństwa, urządzenia poddane modyfikacji Jailbreak nie mogą być używane do bankowości mobilnej.


Sketch
9:41
100%
Witaj!
Aplikacja została zablokowana
z powodu dostępu do root
Z powodów bezpieczeństwa, urządzenia z dostępem do root nie mogą być używane do bankowości mobilnej.



System dodatkowo informuje użytkownika o braku/przywróceniu połączenia z Internetem.




Sketch
9:41
100%
Rejestr autoryzacji
Połączono
37 sekund temu
Przelew błyskawiczny
5 minut. temu
Przelew zwykły
14 minut temu
Logowanie do Bank S.A.
Ponad godzinę temu
Logowanie do Bank S.A.
3 godziny temu
Przelew zwykły
3 godziny temu
Przelew zwykły
Pulpit
Rachunki
Przelew
Koszyk
Więcej

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