



**Bank Spółdzielczy
w Kowalu**

Instrukcja korzystania z aplikacji mobilnej mToken Asseco MAA – klient korporacyjny

Kowal lipiec 2018

Spis treści

1. [Wstęp](#)
2. [Instalacja mToken Asseco MAA](#)
3. [Powiązania urządzenia mobilnego z bankowością elektroniczną](#)
4. [Logowanie](#)
5. [Autoryzacja transakcji](#)
6. [Pulpit aplikacji Asseco MAA](#)
7. [Ustawienie aplikacji Asseco MAA](#)
 - 7.1 [zmiana pin](#)
8. [Dodatki](#)
 - [zablokowanie aplikacji](#)
 - [automatyczne wylogowanie](#)
 - [brak internetu](#)
 - [brak blokady ekranu na urządzeniu mobilnym](#)

1. Wstęp

Aplikacja mobilna mToken Asseco MAA umożliwia autoryzację dyspozycji pochodzących z bankowości internetowej e-bskowal, zarówno transakcji jak i szablonów. Użytkownik zgodnie z poniższą instrukcją dokonuje powiązania urządzenia mobilnego (zainstalowana aplikacja MAA) z bankowością elektroniczną.

2. Instalacja mToken Asseco MAA na urządzeniu mobilnym

Proces pobrania oraz instalacji z portali:

- Google Play  - dla systemu Android 6.x i nowszy

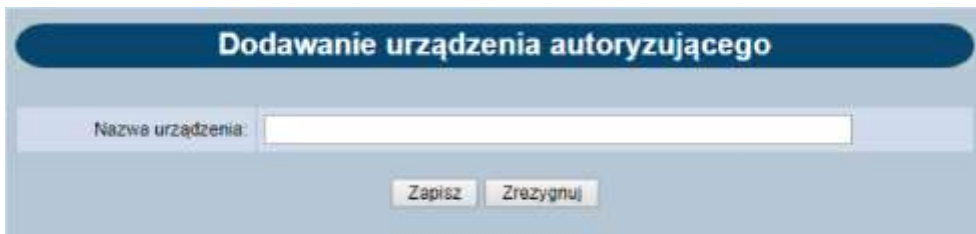
- App Store  - dla systemu iOS 9.x i nowszy

jest analogiczny jak dla każdej innej aplikacji umieszczonej na w/w zasobach. Aplikację mToken Asseco MAA można wyszukać w w/w portalach pod nazwą: **mToken Asseco MAA**

3. Powiązanie urządzenia mobilnego z bankowością elektroniczną

Proces powiązania urządzenia mobilnego (z zainstalowaną aplikacją MAA) z bankowością klienta korporacyjnego można wykonać w następujących krokach:

- a) po zalogowaniu do bankowości elektronicznej dodajemy nowe urządzenie autoryzujące wybierając z menu - w opcji [Urządzenia autoryzujące/Dodaj urządzenie autoryzujące](#) należy podać nazwę własną urządzenia



Dodawanie urządzenia autoryzującego

Nazwa urządzenia:

Zapisz Zrezygnuj

Dodanie urządzenia autoryzującego wymaga potwierdzenia przez administratora klienta korporacyjnego. Do czasu akceptacji przez w/w administratora mobilna autoryzacja nie jest aktywna



Dodawanie urządzenia autoryzującego

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

Zamknij



Nazwa urządzenia	Data powiązania	Status
smartphone	2019-05-28 10:29:04	Czeka na akceptację Administratora

b) Akceptacja dodanego urządzenia autoryzującego przez administratora klienta

- w opcji [Urządzenia autoryzujące/Dodaj urządzenie autoryzujące administracja](#) - administrator może wykonać akceptację (przypisanym środkiem autoryzacji) oczekujące wnioski dotyczące nowych urządzeń autoryzujących

Urządzenia autoryzujące - administracja		
Lista urządzeń autoryzujących - administracja		
Nazwa urządzenia	Data powiązania	Status
smartphone	2018-05-28 10:29:04	Czeka na akceptację Administratora

Po wyborze wskazanego wniosku oczekującego na akceptację, pojawia się formatka szczegółowa z możliwością akceptacji, odrzucenia lub wycofania się z wniosku

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	smartphone
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2018-05-28 10:29:04
Status:	Czeka na akceptację przez Administratora

UWAGA: akceptacja wniosku jest wykonywana przez administratora klienta metodą autoryzacji, która wymaga fizycznego urządzenia (token VASCO lub karta mikroprocesorowa).

Akceptacja urządzenia autoryzującego przez Administratora

Nazwa urządzenia:	smartphone
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2018-05-28 10:29:04
Status:	Czeka na akceptację przez Administratora

Dane do podpisu dla tokena: 7458
9438

Wskazanie tokena:

Zakończona akceptacja zmienia status urządzenia autoryzującego na: *Zaakceptowany przez Administratora* na liście urządzeń

Nazwa urządzenia	Data powiązania	Status
smartphone	2018-05-28 10:29:04	Zaakceptowany przez Administratora

- c) Dokończenie parowania przez użytkownika bankowości korporacyjnej
- w opcji *Urządzenia autoryzujące/Dodaj urządzenie autoryzujące* należy wybrać zaakceptowane przez administratora klienta urządzenie oraz uruchomić opcję: *Dokończ dodawania urządzenia*

Urządzenie autoryzujące - szczegóły

Nazwa urządzenia:	smartphone
Producent:	
Platforma:	
Wersja:	
Model:	
Data powiązania:	2018-05-28 10:29:04
Status:	Zaakceptowany przez Administratora

Dokończ dodawanie urządzenia
Usuń
Zrezygnuj

- jako potwierdzenie poprawnego dodania nowego urządzenia autoryzującego, bankowość korporacyjna wyświetli potwierdzenie dodania urządzenia oraz dodatkowe informacje:
 - kod aktywacyjny – kod będzie użyty podczas powiązania mToken Asseco MAA z bankowością korporacyjną
 - informację o wysłaniu kodu SMS na wskazany nr telefonu
 - termin ważności wygenerowanego kodu (5 minut)

Dodawanie urządzenia autoryzującego

Kod aktywacyjny: **539598**

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

W trakcie aktywowania usługi w urządzeniu mobilnym zostaniesz poproszona/poproszony o podanie kodu weryfikacyjnego, który zostanie wysłany za pomocą SMS na numer: **48691532532**.

Kod jest ważny przez 5 minut.

Pozostań na stronie i dokończ proces aktywacji na urządzeniu autoryzującym.



Oczekiwanie na zakończenie procesu aktywacji.

Zamknij

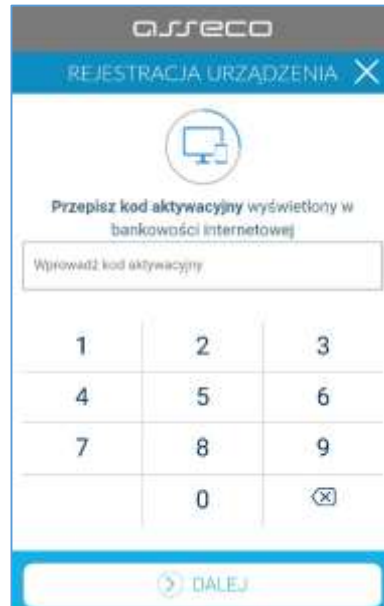
- d) Powiązanie aplikacji mobilnej z bankowością korporacyjną
- po uruchomieniu aplikacji mToken Asseco MAA na urządzeniu mobilnym należy wykonać rejestrację urządzenia

- po uruchomieniu aplikacji mToken Asseco MAA na urządzeniu mobilnym należy wykonać rejestrację urządzenia



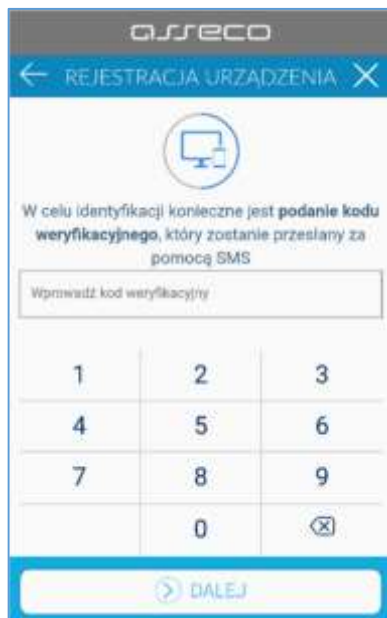
ekran rejestracji urządzenia w mToken Asseco MAA

- w pierwszym kroku rejestracji należy wprowadzić poprawny **kod aktywacyjny** wygenerowany w bankowości elektronicznej



wprowadzenie kodu weryfikacyjnego

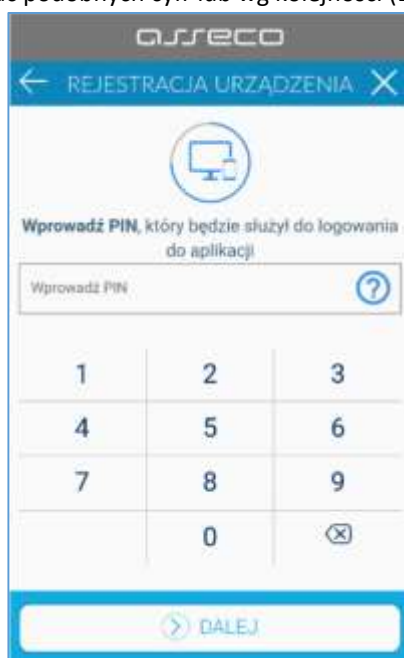
- w kolejnym kroku w celu identyfikacji należy wprowadzić kolejny kod SMS otrzymany na wskazany nr telefonu



wprowadzenie dodatkowych danych weryfikacyjnych

- w następnym kroku w polu należy wprowadzić kod PIN, który będzie służył do logowania w aplikacji mToken Asseco MAA. Nadawany nr PIN ma następujące właściwości:

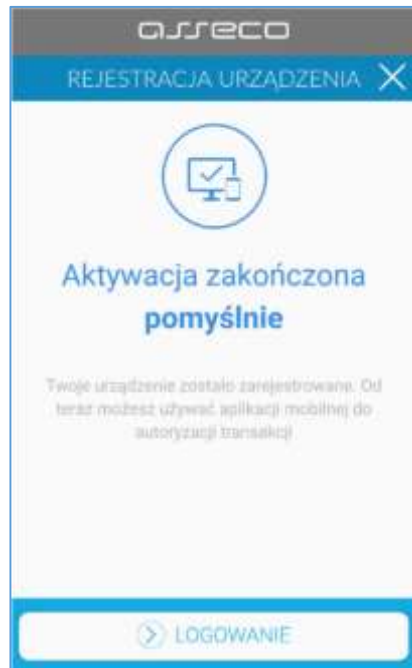
- musi zawierać od 5 do 8 cyfr,
- nie może zawierać podobnych cyfr lub wg kolejności (11111, 22222, 123123, 12345, itp.)



wprowadzenie PIN-u

- w kolejnym kroku należy ponownie wprowadzić kod PIN. System kontroluje prawidłowość i zgodność zdefiniowanego kodu PIN

- po poprawnym wprowadzeniu kodu PIN, mToken Asseco MAA informuje o pozytywnej aktywacji



potwierdzenie poprawnie wykonanej aktywacji

- po poprawnej aktywacji urządzenia użytkownik zostanie przekierowany na ekran główny aplikacji MAA, poprzez który będzie miał możliwość zalogowania się do aplikacji mobilnej za pomocą kodu PIN zdefiniowanego w procesie rejestracji urządzenia autoryzującego.

4. Logowanie

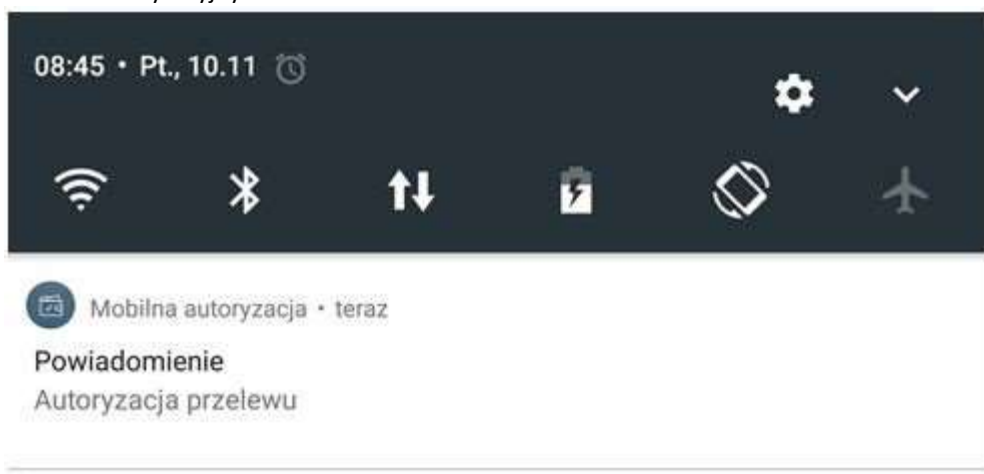
- w celu zalogowania się do aplikacji mobilnej Asseco MAA należy podać PIN oraz wybrać przycisk [ZALOGUJ]. Na ekranie dodatkowo prezentowana jest informacja o banku **BS KOWAL** oraz identyfikator (login) użytkownika, który jest częściowo zamaskowany.



5. Autoryzacja transakcji

- w systemie bankowości elektronicznej po przekazaniu do zatwierdzenia transakcji prezentowany jest ekran informujący o wysłaniu dyspozycji do autoryzacji na aplikację mobilną Asseco MAA poprzez powiadomienie PUSH.

- w aplikacji mobilnej wyświetlany jest na urządzeniu baner powiadomienia PUSH z informacją o oczekującym powiadomieniu autoryzacyjnym.



- wybieramy baner powiadomienia PUSH, które uruchamia aplikację Asseco MAA lub bezpośrednio uruchamiamy aplikację z systemu operacyjnego urządzenia mobilnego.
- loguje się do aplikacji Asseco MAA za pomocą kodu PIN



- w aplikacji prezentowane są dane dyspozycji do autoryzacji, w celu przejścia na ekran potwierdzenia operacji należy wybrać przycisk [AKCEPTUJ].



- wybór przycisku [ODRZUĆ] powoduje odrzucenie potwierdzenia autoryzacji
- wybór przycisku [AKCEPTUJ] wymusza podanie PINU i potwierdzeniu przyciskiem [ZATWIERDŹ]



- po poprawnym zatwierdzeniu operacji pojawia się okienko informacyjne „Operacja zakończona”



- a w systemie bankowości internetowej e-bkował zostanie zaprezentowany komunikat o zatwierdzeniu/odrzuconiu autoryzacji dyspozycji.

6. Pulpit aplikacji Asseco MAA

Po zalogowaniu się do aplikacji Asseco MAA zostanie wyświetlony pulpit prezentujący listę **Autoryzacje**, listę **Powiadomienia** lub listę **Ustawienia**.

Na ekranie wyświetlana jest lista autoryzacji lub lista powiadomień, które otrzymał użytkownik. W celu wyświetlenia kolejnych autoryzacji/powiadomień należy przewinąć listę w górę/dół.

AUTORYZACJE



07.05.2018

Depozyt rentierski 6 - miesięcz...



07.05.2018

123456aaaaaaaa



07.05.2018

Przelew testowy



07.05.2018

Realizacja przelewu



07.05.2018



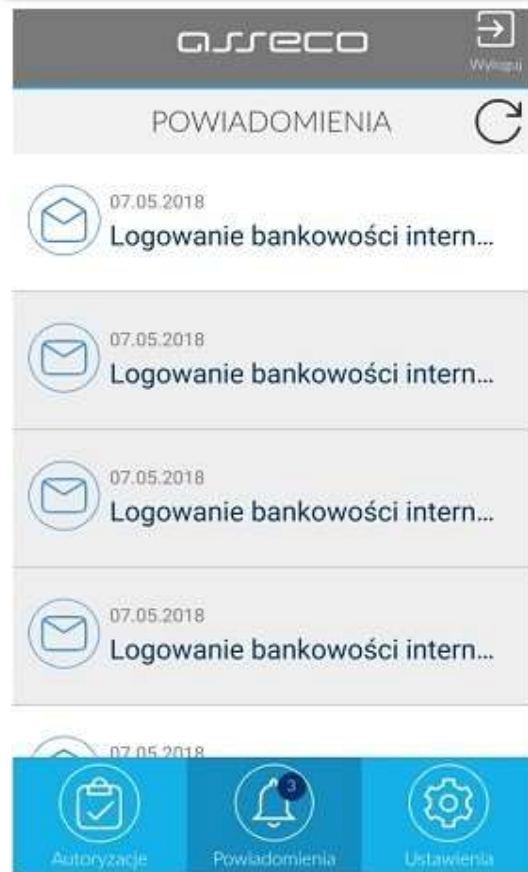
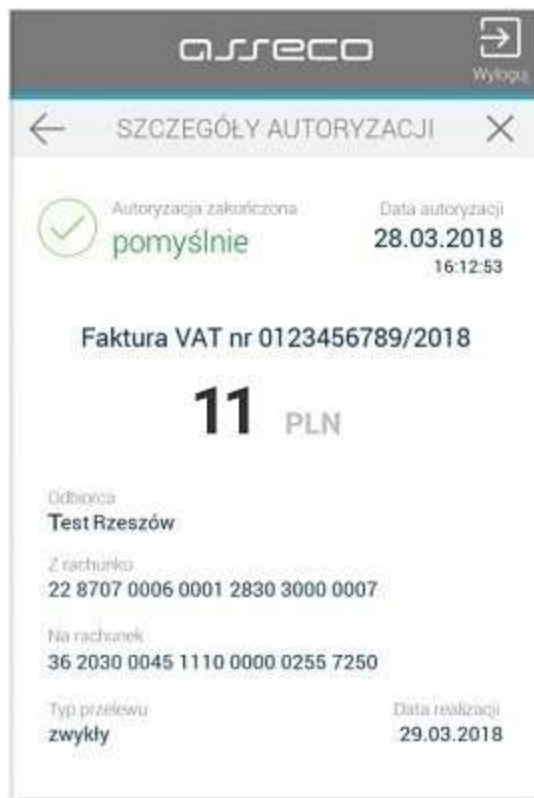
Autoryzacje



Powiadomienia




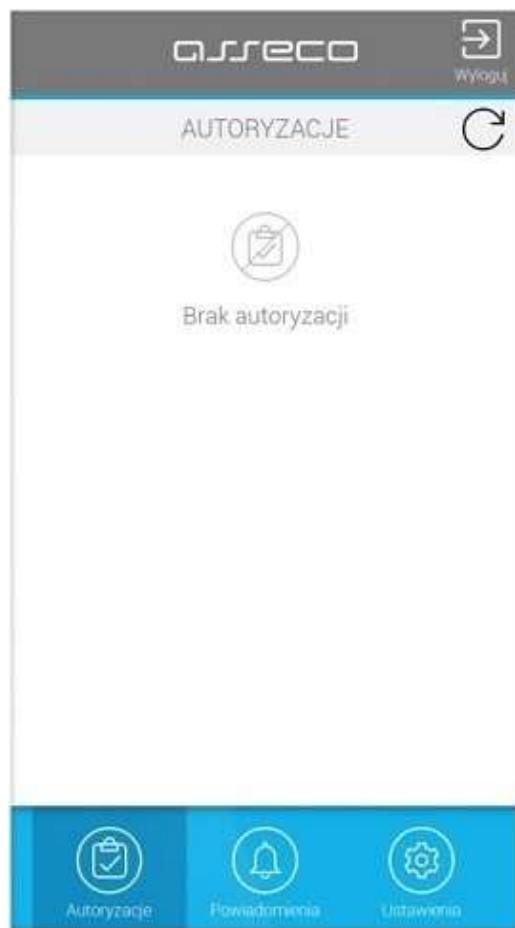
Ustawienia



Wybór pozycji na widoczce **Autoryzacje/Powiadomienia** przenosi użytkownika do podglądu szczegółów autoryzacji/powiadomienia.



Ikonka  dostępna na widżecie **Autoryzacje** oraz **Powiadomienia** umożliwia odświeżanie prezentowanej listy. W przypadku, gdy użytkownik nie posiada autoryzacji/powiadomień na widżecie prezentowany jest odpowiedni komunikat jak na poniższym ekranie.





7. Ustawienia aplikacji Asseco MAA

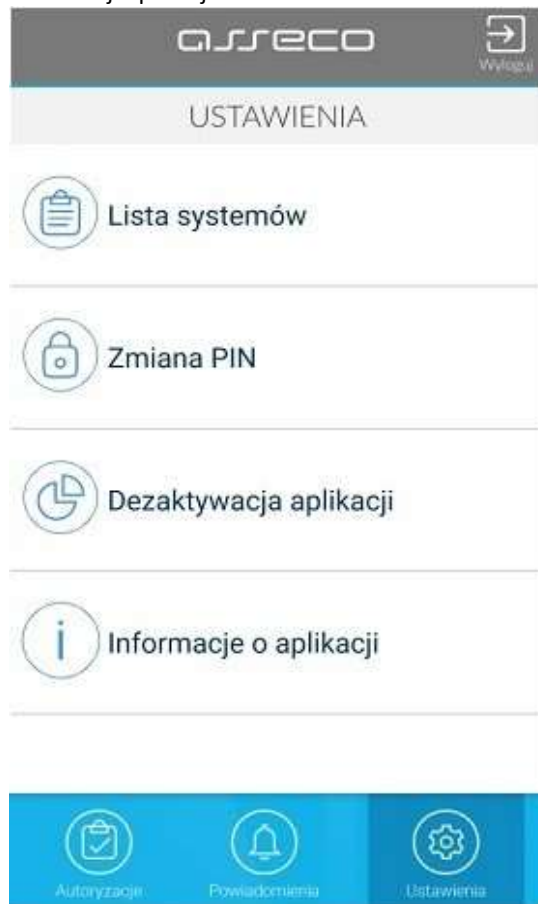
Po zalogowaniu do aplikacji i wybraniu na widżecie pozycji **Ustawienia** wyświetlona jest lista opcji:

Lista systemów - BS KOWAL

Zmiana PIN- możliwość zmiany PIN

Dezaktywacja aplikacji – możliwość dezaktywacji aplikacji

Informacja o aplikacji - nazwa i numer wersji aplikacji



Opcja **informacja o aplikacji** prezentuje informacje szczegółowe o aplikacji Asseco MAA.



Opcja **dezaktywacja aplikacji** umożliwi dezaktywację aplikacji Asseco MAA. W tym celu należy kliknąć w przycisk [DEZAKTYWUJ APLIKACJĘ].



7.1 . Zmiana pinu w aplikacji Asseco MAA

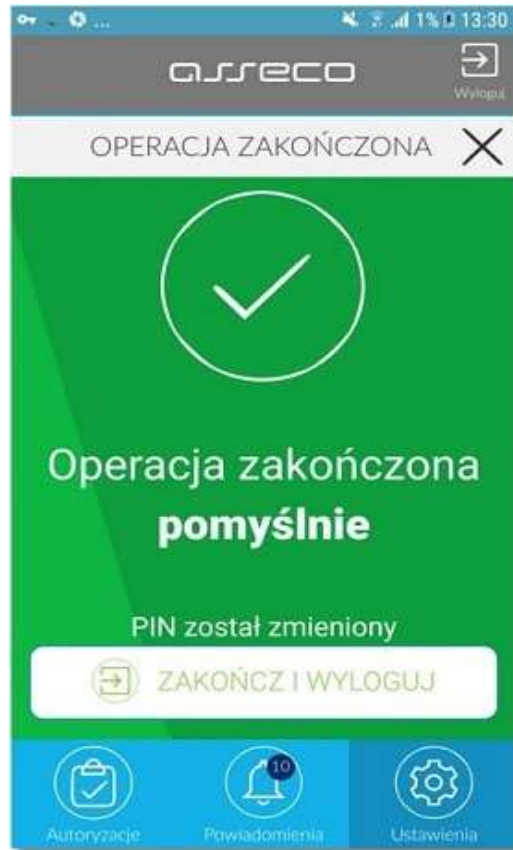
Opcja umożliwia użytkownikowi zmianę obecnego kodu PIN do aplikacji Asseco MAA na inny.

The screenshot shows the 'ZMIANA PIN' screen in the Asseco MAA application. The interface includes a header with the 'asseco' logo and a 'Wyloguj' button. The main area is titled 'Zmień PIN:' and features two input fields: 'Wprowadź obecny PIN' and 'Wprowadź nowy PIN' (with an eye icon for visibility). Below these fields is a numeric keypad with digits 1-9, 0, and a delete icon. A 'ZATWIERDŹ' button with a checkmark icon is positioned below the keypad. The bottom navigation bar contains three icons: 'Autoryzacje', 'Powiadomienia', and 'Ustawienia'.

W celu zmiany kodu PIN użytkownik w polu **Wprowadź obecny PIN** wprowadza aktualny PIN, którym się loguje do aplikacji Asseco MAA a następnie w polu **Wprowadź nowy PIN** wprowadza nowy kod PIN.


This screenshot shows the same 'ZMIANA PIN' screen as the previous one, but the input fields are now masked with dots. The 'Wprowadź obecny PIN' field contains four dots, and the 'Wprowadź nowy PIN' field contains six dots. The rest of the interface, including the numeric keypad and the 'ZATWIERDŹ' button, remains the same.

Po poprawnej zmianie kodu PIN i zatwierdzeniu przyciskiem [ZATWIERDŹ], system informuje o zakończeniu operacji.



W przypadku, gdy użytkownik w polu **Wprowadź obecny PIN** wprowadzi błędny aktualny kod PIN a następnie w polu **Wprowadź nowy PIN** wpisze nowy kod PIN i zatwierdzi przyciskiem [ZATWIERDŹ], system poinformuje o odrzuceniu operacji.



Przycisk z ikonką  powoduje, że znaki w polu **Wprowadź nowy PIN** są niemaskowane.



Pole **Wprowadź nowy PIN** nie może być puste.



PIN musi posiadać od 5 do 8 cyfr.



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 stosowny komunikat walidacyjny



8. Dodatki

a) Zablokowanie aplikacji

- aplikacja zabezpieczona jest przed wielokrotnym wprowadzeniem błędnego kodu PIN.



The screenshot shows the login interface of the GJSECO application. At the top, there is a grey header with the GJSECO logo and a blue bar with the word "LOGOWANIE". Below this, the user's name "BS Kowal" and account type "Kierca indywidualna" are displayed on the left, and the account number "(KG****5)" is on the right. The main instruction is "Podaj PIN, aby się zalogować". There is a text input field labeled "Wprowadź PIN" and a numeric keypad with digits 1-9, 0, and a clear button. At the bottom, there is a blue button labeled "ZALOGUJ".

- po przekroczeniu liczby błędnie wprowadzonych kodów PIN zostanie zaprezentowany komunikat jak na poniższym ekranie.



The screenshot shows the application blocked screen. At the top, there is a grey header with the GJSECO logo and a blue bar with the text "APLIKACJA ZABLOKOWANA". In the center, there is a large red circle with a red 'X' inside. Below this, the text "Aplikacja została zablokowana" is displayed in red. Underneath, a message explains: "Przekroczono limit błędów logowań. W celu uruchomienia aplikacji należy ponownie zarejestrować urządzenie w bankowości internetowej". At the bottom, there is a blue button labeled "REJESTRUJ PONOWNIE".

- w takim przypadku, konieczne będzie ponowne powiązanie urządzenia mobilnego z systemem bankowości internetowej (zgodnie z punktem 3 tej instrukcji)

b) automatyczne wylogowanie po 10 sekundach

- w przypadku, gdy użytkownik będąc zalogowanym do aplikacji Asseco MAA przejdzie (bez wcześniejszego wylogowania się) do innych funkcji dostępnych na urządzeniu mobilnym, a następnie wróci ponownie do aplikacji Asseco MAA wówczas po upływie co najmniej 10 sekund nastąpi wylogowanie z aplikacji. W takiej sytuacji użytkownik będzie musiał odblokować aplikację Asseco MAA poprzez ponowne wprowadzenie kodu PIN oraz wybór przycisku [ODBLOKUJ].

The image shows a mobile application interface for PIN entry. At the top, the name 'BS KOWAL' is displayed. Below it is a text input field with the placeholder 'Wprowadź PIN'. Underneath is a numeric keypad with digits 1 through 9, 0, and a backspace icon. At the bottom is a large button labeled 'ODBLOKUJ'.

c) brak internetu

- W przypadku braku połączenia z internetem po uruchomieniu aplikacji Asseco MAA prezentowany jest stosowny komunikat informacyjny wraz z przyciskiem [SPRAWDŹ PONOWNIE] W momencie przywrócenia dostępu do internetu przycisk [SPRAWDŹ PONOWNIE] umożliwi przejście do ekranu logowania aplikacji Asseco MAA.



d) brak blokady ekranu na urządzeniu mobilnym

- w systemie Asseco MAA zastosowana jest kontrola, czy urządzenie autoryzujące posiada blokadę ekranu. Po uruchomieniu aplikacji, w przypadku braku blokady zostanie zaprezentowany komunikat jak na poniższym ekranie. W takiej sytuacji należy ustawić kod PIN dla urządzenia lub hasło blokady ekranu.

