ZMIANY W LOGOWANIU I AUTORYZACJI BANKOWOŚCI INTERNETOWEJ

W związku z wdrożeniem Dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2015/2366 z dnia 25 listopada 2015 roku (PSD2) w sprawie usług płatniczych w ramach rynku wewnętrznego nałożono na banki obowiązek wzmocnienia bezpieczeństwa autoryzacji transakcji. **Zmiany o których mowa dotyczą zarówno procesu autentykacji (logowania) jak i procesu autoryzacji (podpisu).** Aby podnieść standardy bezpieczeństwa banki zobligowane są stosować silne uwierzytelnienie, które wymaga co najmniej 2 niezależnych elementów niezbędnych do logowania/autoryzacji.

Wykonywanie operacji dotychczasowymi metodami nie będzie możliwe po 14 września 2019. **Zapraszamy do kontaktu z pracownikami naszego Banku w celu wprowadzenia zmian w Państwa dostępie do bankowości internetowej.** Sugerujemy jak najszybsze złożenie wniosku o zmianę sposobu autoryzacji na mToken Asseco MAA lub SMS autoryzacyjny. Nadmieniamy, że aktywacja i użytkowanie Tokena Asseco MAA są bezpłatne.

Użytkownicy tokena RSA powinni udać się do najbliższej placówki Banku w celu dokonania formalności związanych ze zmianą formy autoryzacji. Z kolei użytkownicy haseł stałych/maskowanych, kodów SMS, tokena mobilnego Asseco MAA i karty mikroprocesorowej nie muszą podejmować żadnych działań - zmiany w autoryzacji dokonają się automatycznie.

Poniżej prezentujemy tabele zawierającą zestawienie dotychczasowych oraz nowych metod autentykacji (logowania) i autoryzacji (podpisu) z podziałem na klienta indywidualnego. **Poniżej tabeli prezentujemy szczegółowe informacje dotyczące konkretnego wariantu.**

Zmiany dotyczące KLIENTA INDYWIDUALNEGO (system Asseco CBP)

	Przed zmianami		**Po zmianach**	
Numer wariantów	**Obecna autentykacja**	**Obecna autoryzacja**	**Nowa autentykacja**	**Nowa autoryzacja**
Wariant nr 1	Hasło maskowane	Kod SMS	Hasło maskowane + Kod SMS	Kod SMS + PIN[1]
Wariant nr 2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + Token mobilny Asseco MAA + PIN[2]	Token mobilny Asseco MAA + PIN[2]
Wariant nr 3	Hasło stałe + Token RSA	Hasło stałe + Token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN[1]
			Hasło maskowane + Token mobilny Asseco MAA + PIN[2]	Token mobilny Asseco MAA + PIN[2]

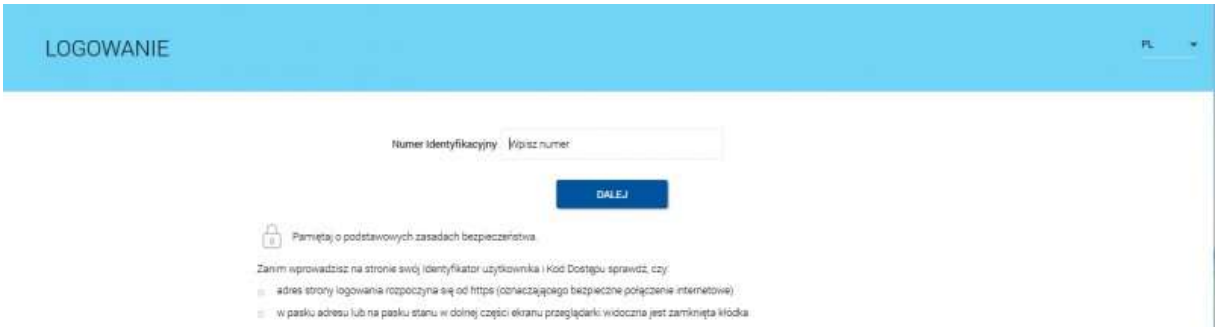
Legenda:

1 - kod PIN autoryzujący. Klient zostanie poproszony o utworzenie PINu autoryzującego podczas pierwszej autoryzacji zlecenia.

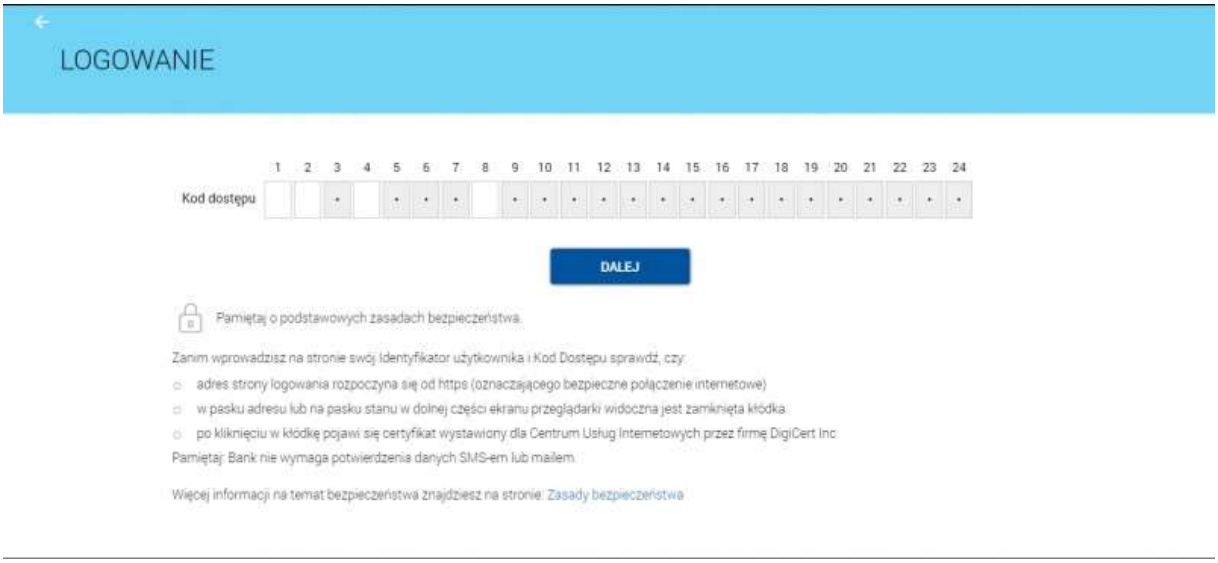
2 - kod PIN służący do logowania do aplikacji mToken mobilny Asseco MAA

Wariant nr 1

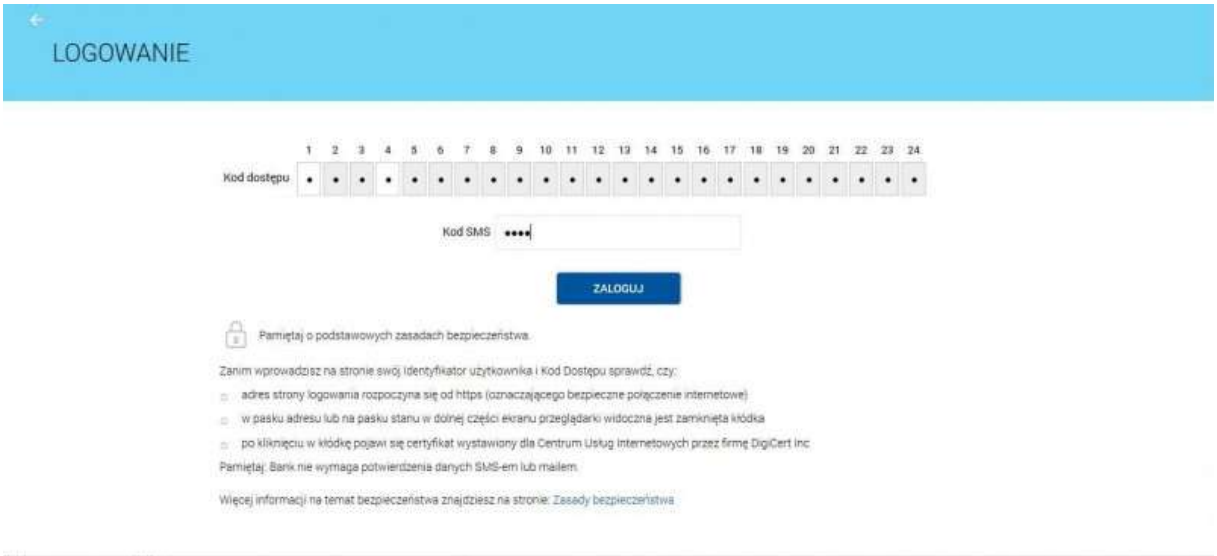
Wprowadzenie identyfikatora użytkownika:



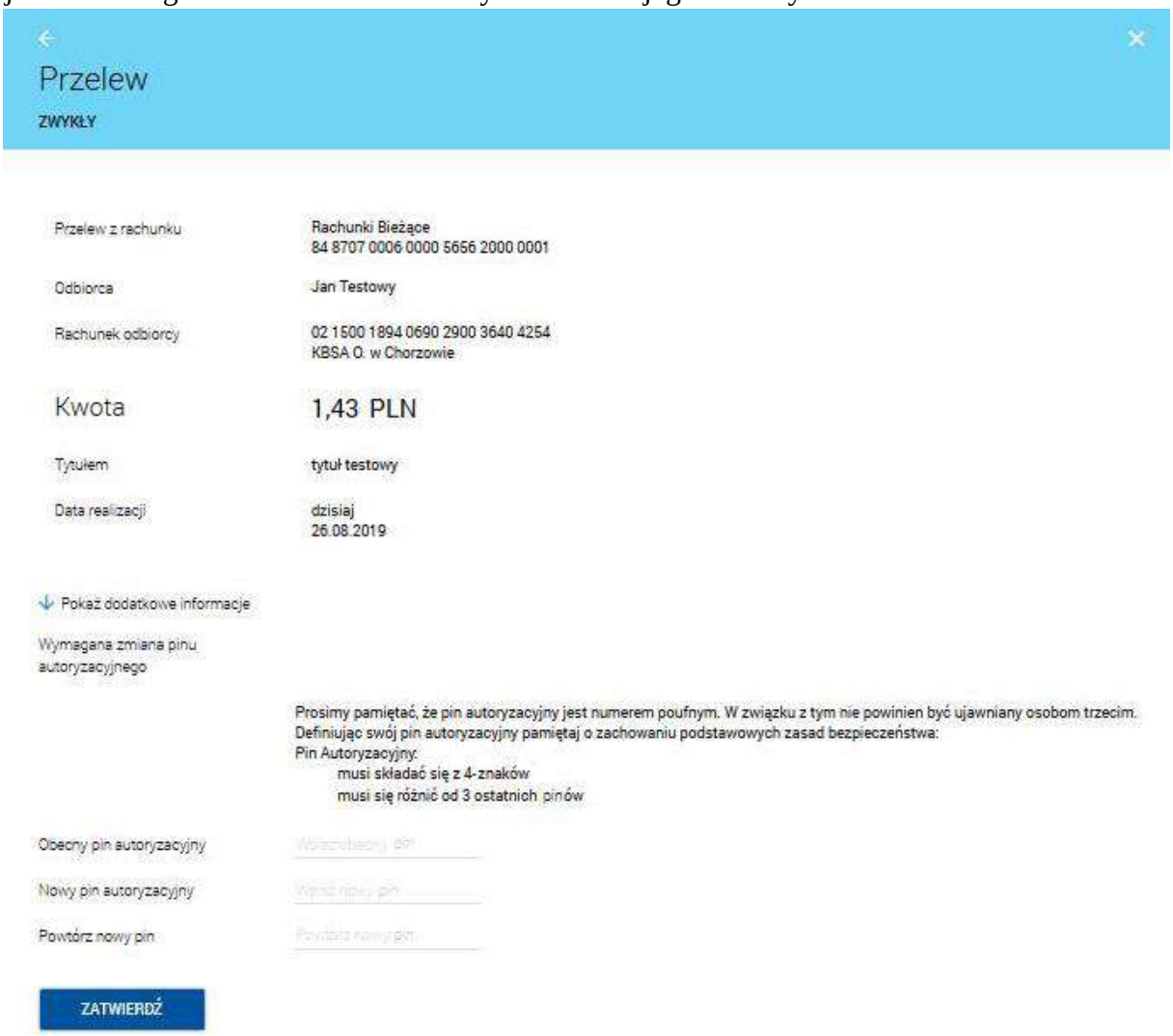
Wprowadzenie hasła maskowanego:



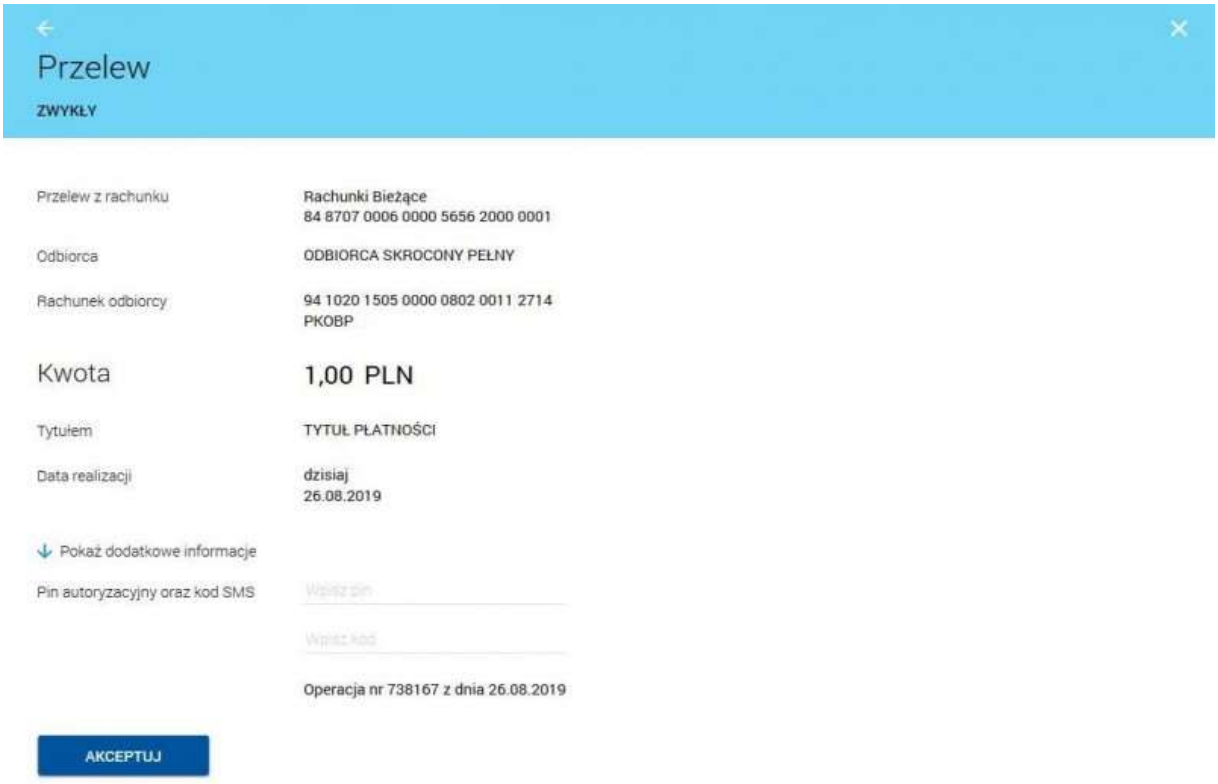
Wprowadzenie kodu SMS:



Tylko pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany:



Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS:

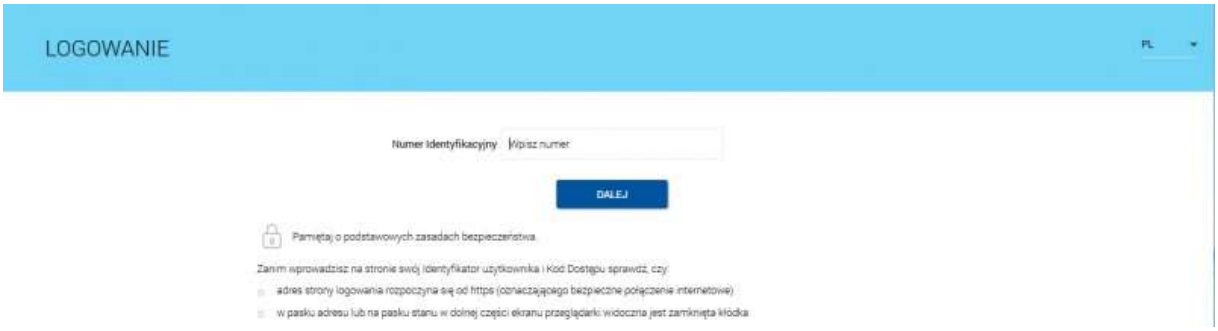


Wariant nr 2

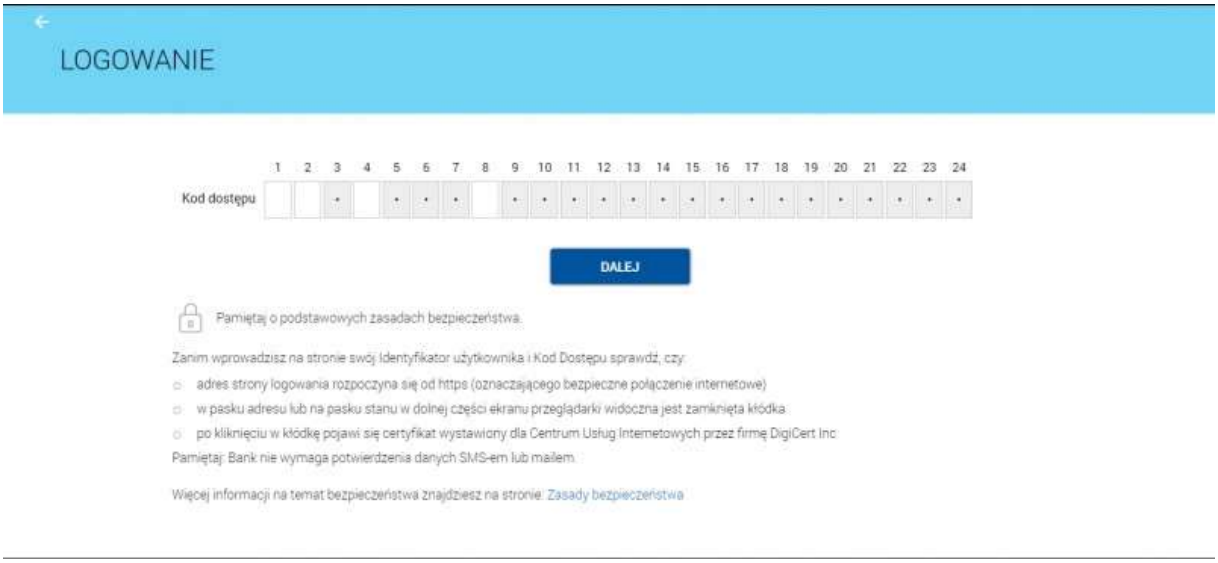
Użytkownicy korzystający z hasła maskowanego i tokena mobilnego Asseco MAA nie muszą odwiedzać naszych placówek - zmiany w sposobie autoryzacji dokonają się automatycznie.

AUTENTYKACJA:

Wprowadzenie identyfikatora użytkownika:

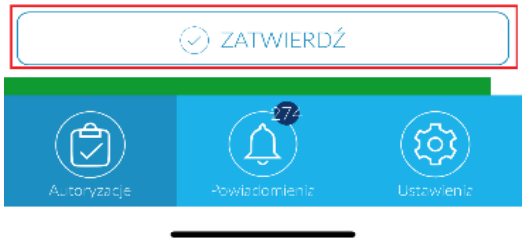


Wprowadzenie hasła maskowanego:



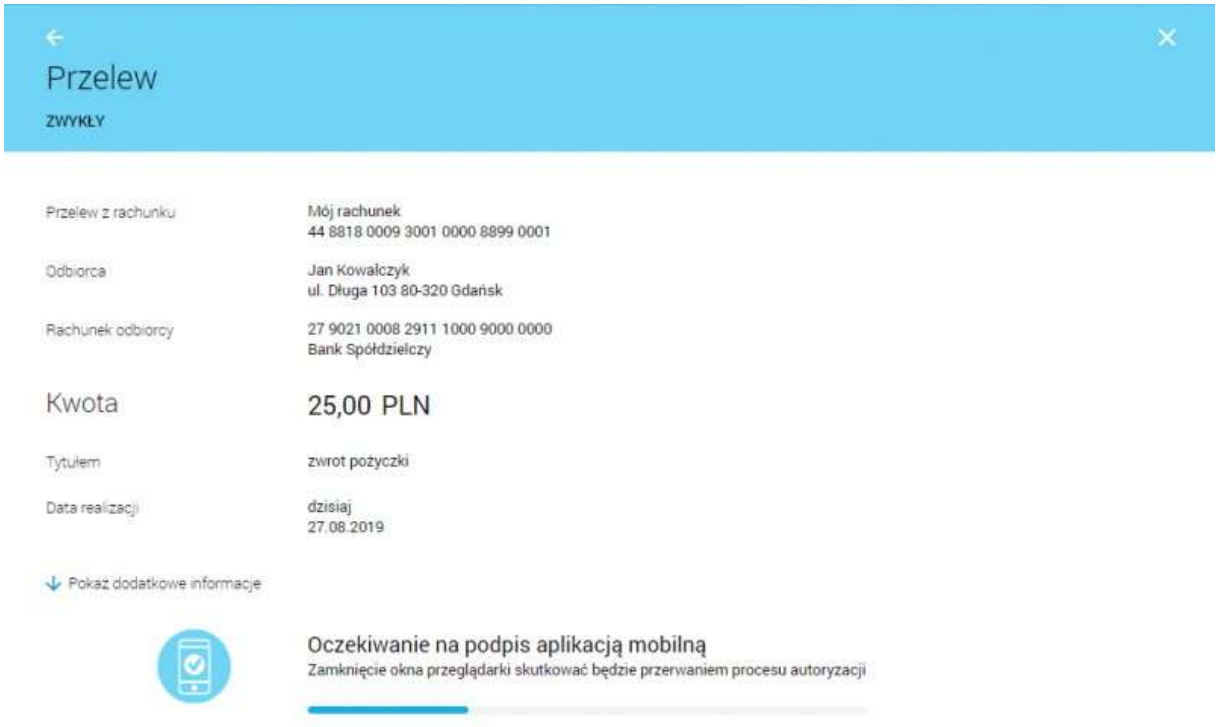
Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:

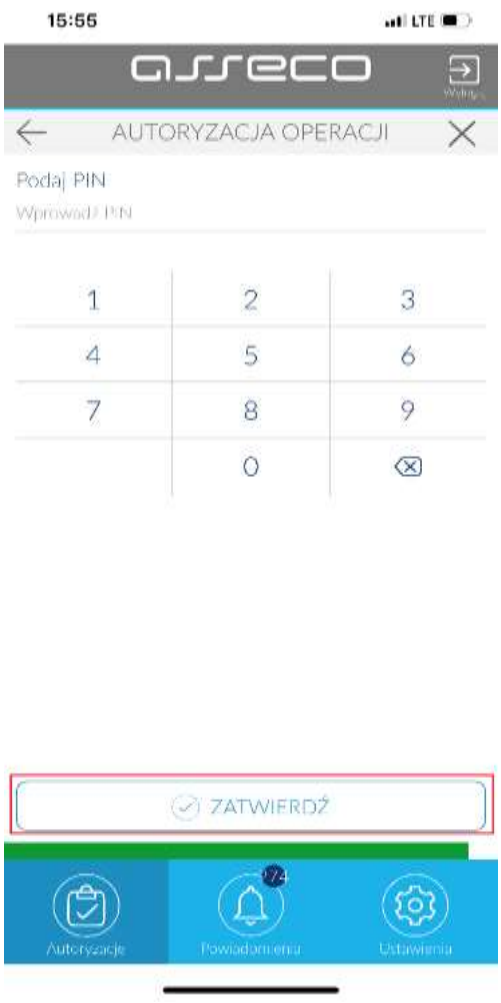


AUTORYZACJA:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem w procesie autoryzacji:



Wariant nr 3

W przypadku użytkowników tokena RSA konieczna jest wizyta w najbliższej placówce Banku w celu zmiany metody autoryzacji - WARIANT 1 lub WARIANT 2.