Zmiany w bankowości CBP (ebank.bsszczytno.pl)

1. Wstęp – dostosowanie środków dostępu użytkowanych w CUI do wymogów silnego uwierzytelniania (SCA)

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostaną uzupełnione o dodatkowe wymagania SCA (tzw.: „silne uwierzytelnienie klienta"). „Silne uwierzytelnianie klienta" oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.
Dostosowanie do wymogów SCA dotyczy procesu autentykacji (logowania) oraz autoryzacji (podpisu).

Planowanie termin wprowadzenia zmian to 11.09.2019 r, lecz nie później niż 14.09.2019r.

2. CBP – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w poniższej tabeli:

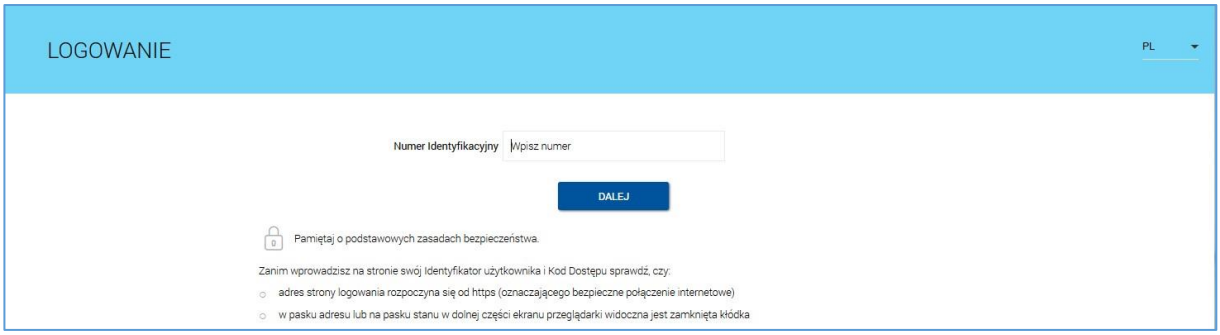
	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
Nr schematu „autentykacja - autoryzacja"	**Obecna autentykacja**	**Obecna autoryzacja**	**Nowa autentykacja**	**Nowa autoryzacja**
1	Hasło maskowane	Kod SMS	Hasło maskowane + kod SMS	Kod SMS + PIN
2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

2.1. Opis szczegółowy – Hasło maskowane, Kod SMS

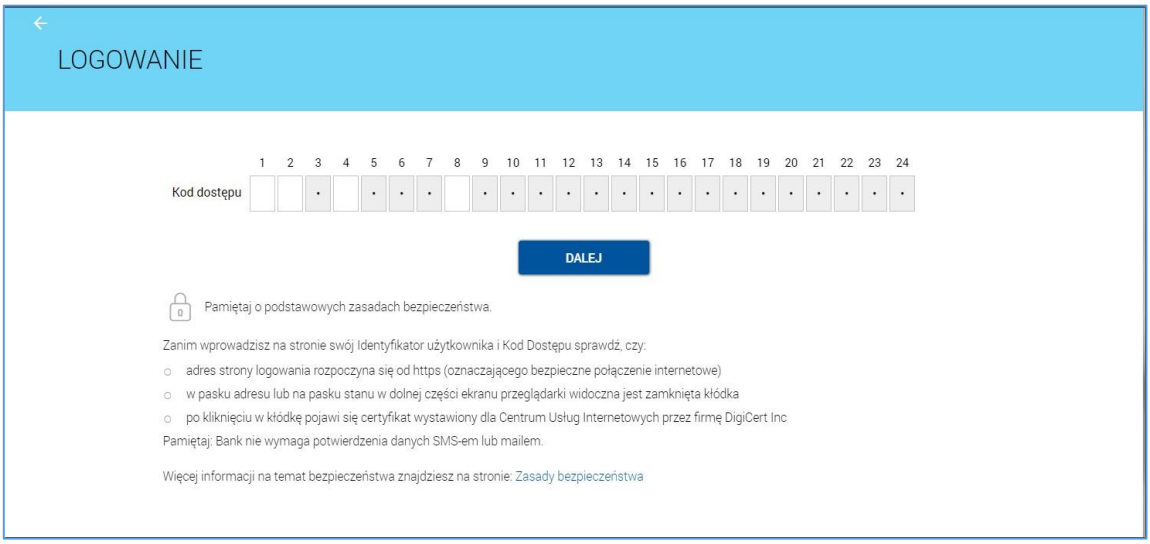
Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) Autentykacja (logowanie):

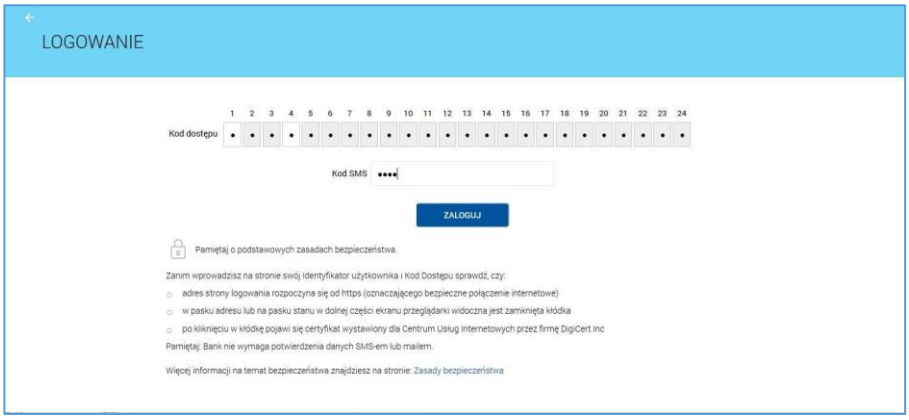
Wprowadzenie identyfikatora użytkownika:



Wprowadzenie hasła maskowanego:

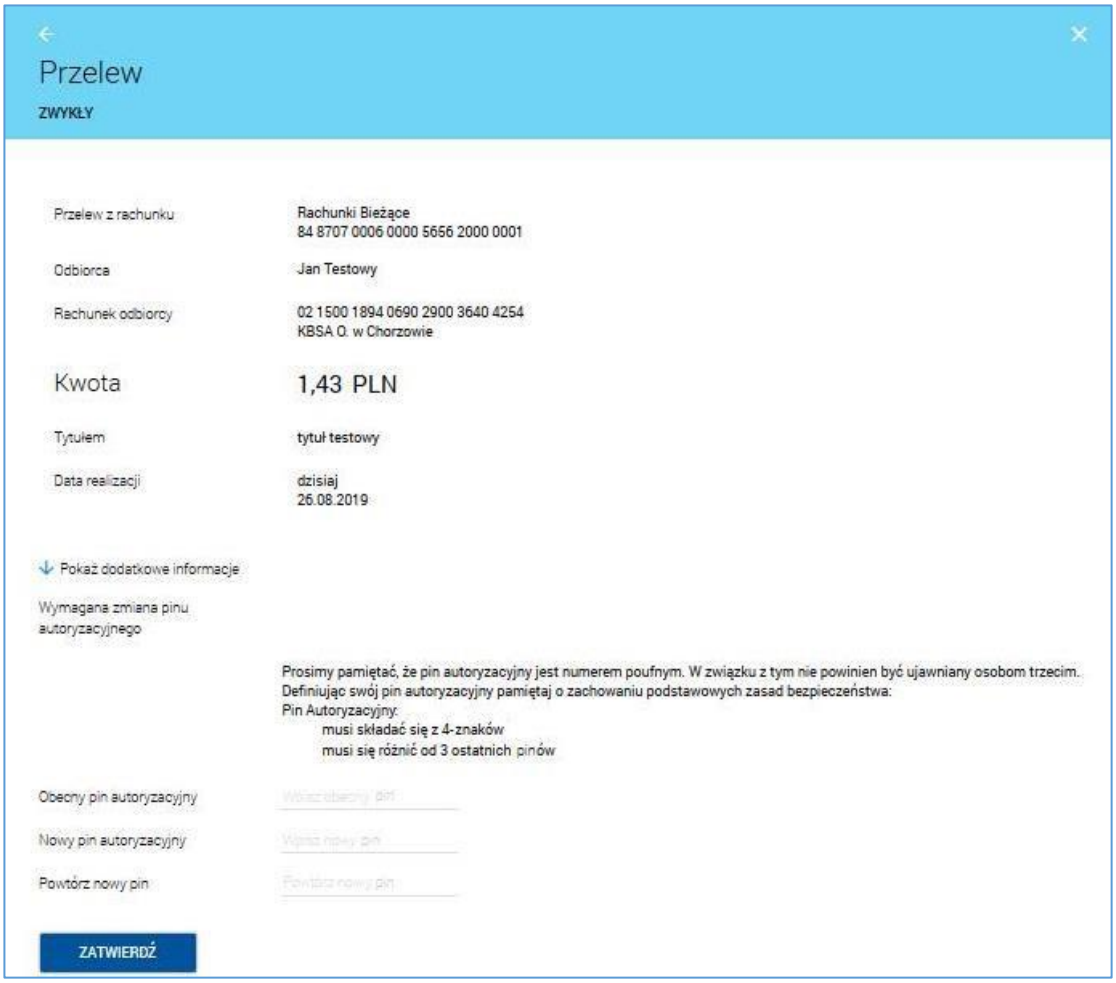


Wprowadzenie kodu SMS:

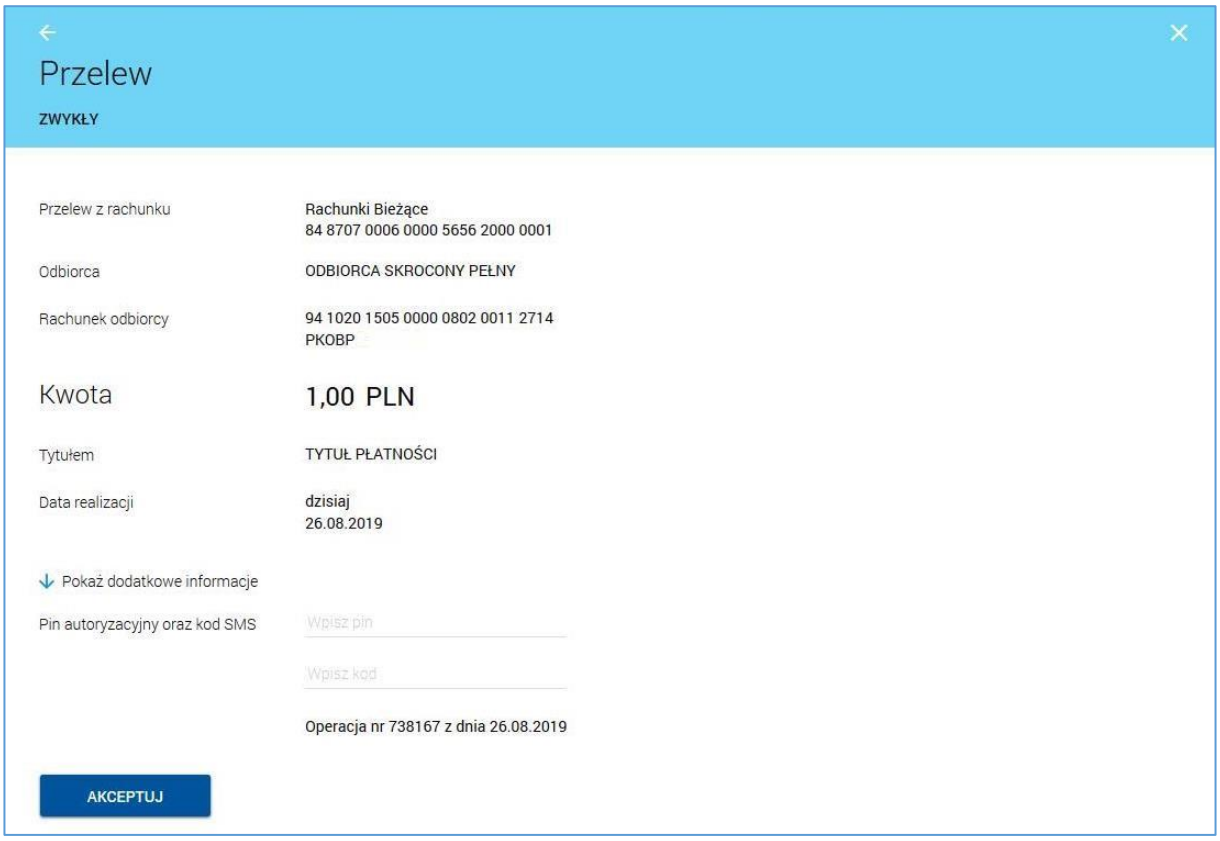


ii) Autoryzacja (podpisywanie):

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:

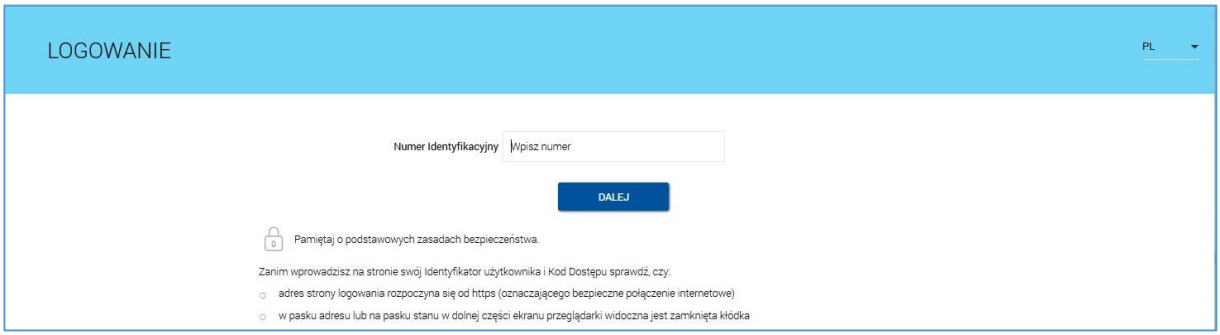


2.2. Opis szczegółowy - Hasło maskowane, mToken

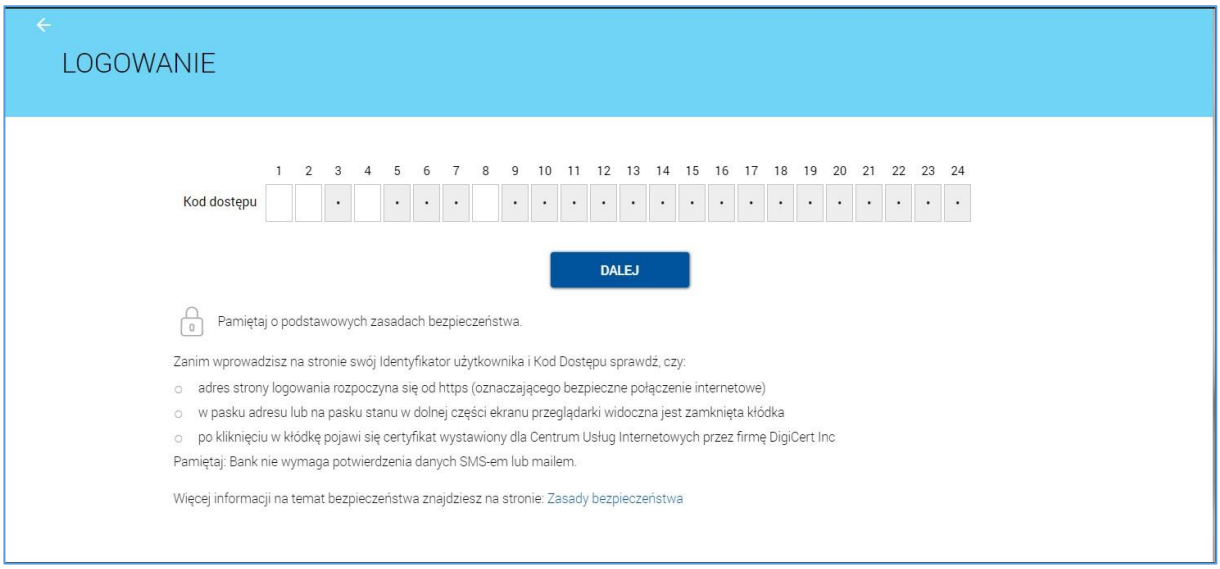
Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) Autentykacja (logowanie):

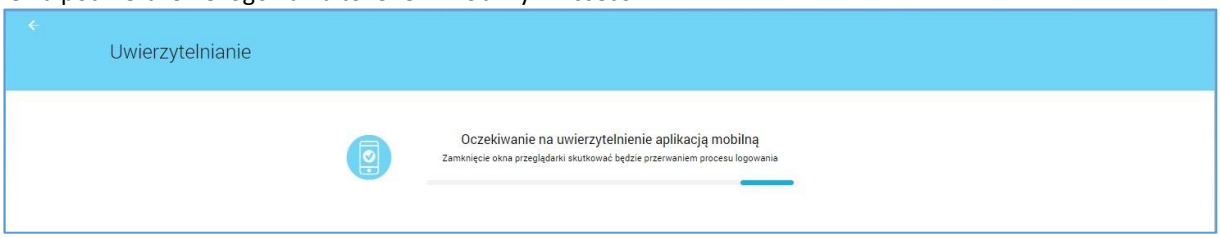
Wprowadzenie identyfikatora użytkownika:



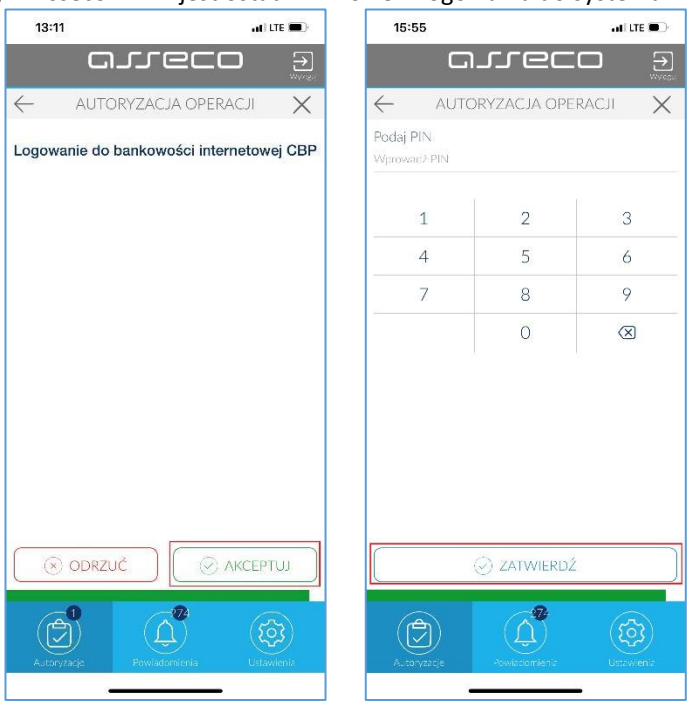
Wprowadzenie hasła maskowanego:



Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

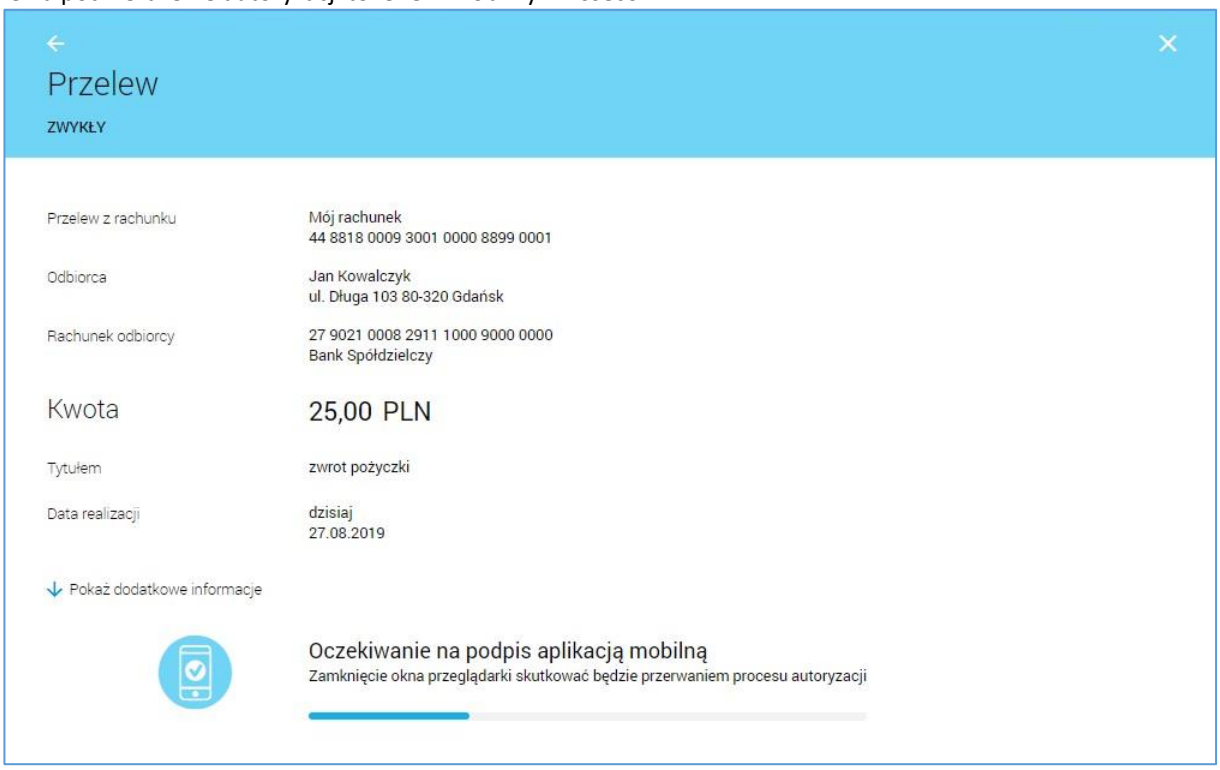


Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:

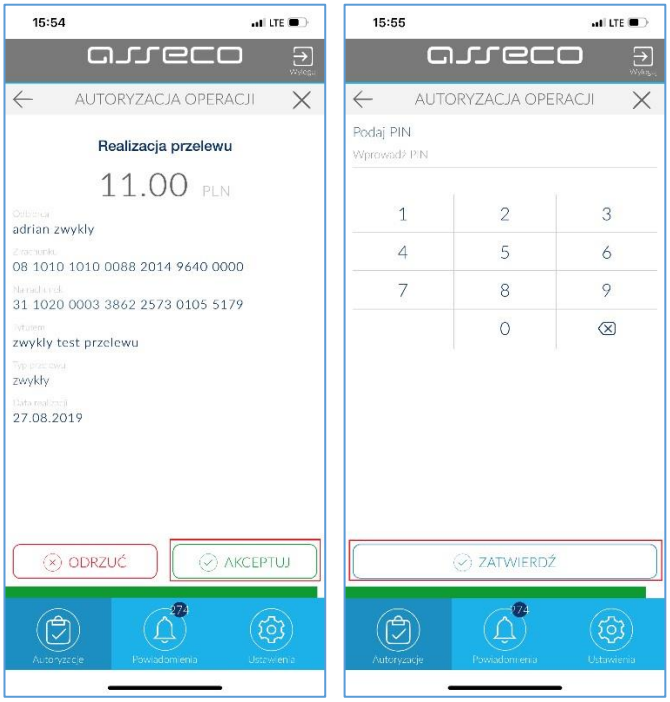


ii) Autoryzacja (podpisywanie):

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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



Pozostałe funkcjonalności bankowości nie ulegają zmianom.