Bank Spółdzielczy
w Dołhobyczowie

Dostosowanie środków dostępu użytkowanych w systemach bankowości elektronicznej detalicznej Asseco CBP wymagań SCA (silne uwierzytelnianie)

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

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostały 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).

W/w zasada (SCA) determinuje zmiany w obecnie użytkowanych schematach środków dostępu, tj.:

<u>Bankowość detaliczna – Asseco CBP</u>

- autentykacja: hasło maskowane, autoryzacja: kod SMS
- autentykacja: hasło maskowane, autoryzacja: token mobilny Asseco MAA
- autentykacja: hasło stałe + token RSA, autoryzacja: hasło stałe + token RSA
- autentykacja: hasło maskowane, autoryzacja: token RSA

2. Asseco CBP – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w tabeli 1:

Tabela 1	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
3	Hasło stałe + token RSA	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN
4	Hasło maskowane	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

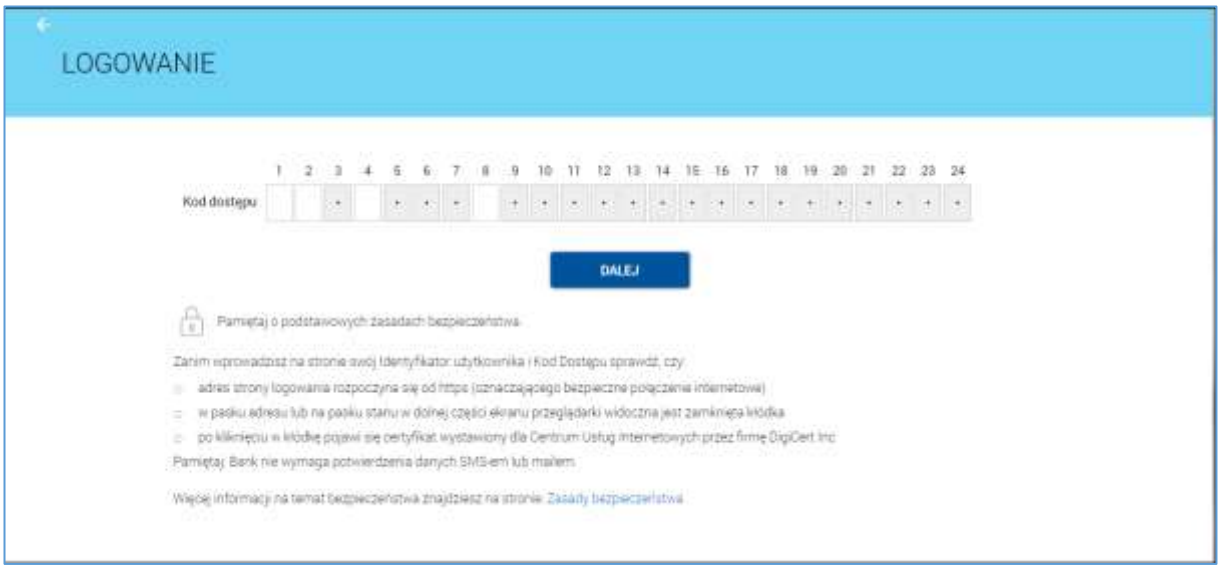
2.1. Opis szczegółowy – schemat nr 1 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Kod SMS)

a) Wygląd formatek dla użytkownika po wprowadzeniu SCA

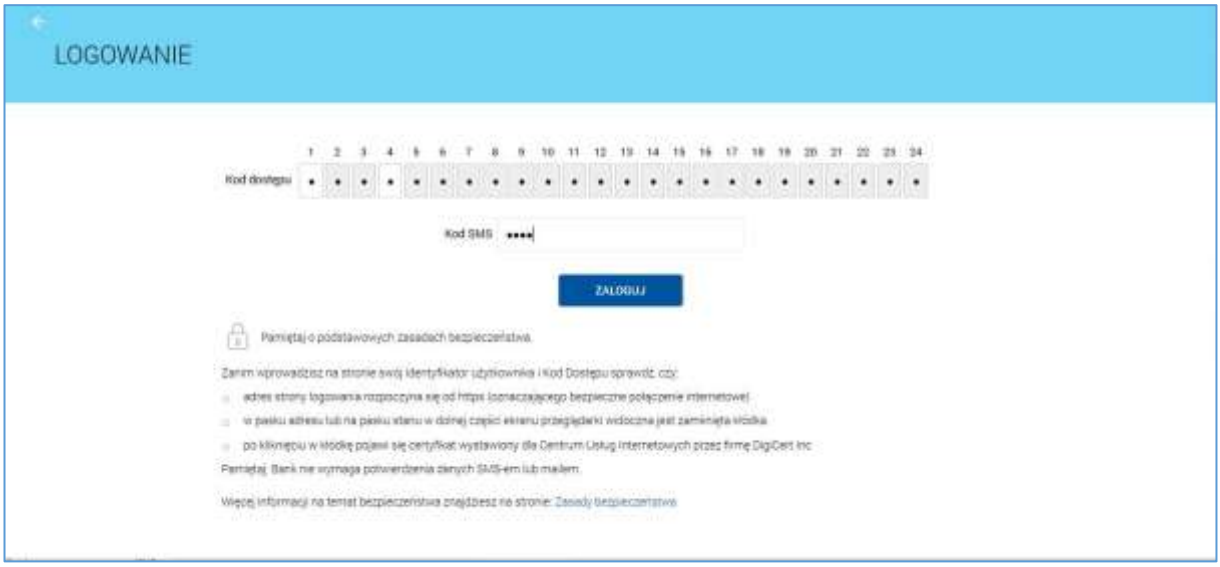
i) autentykacja:

Wprowadzenie identyfikatora użytkownika:

Wprowadzenie hasła maskowanego:

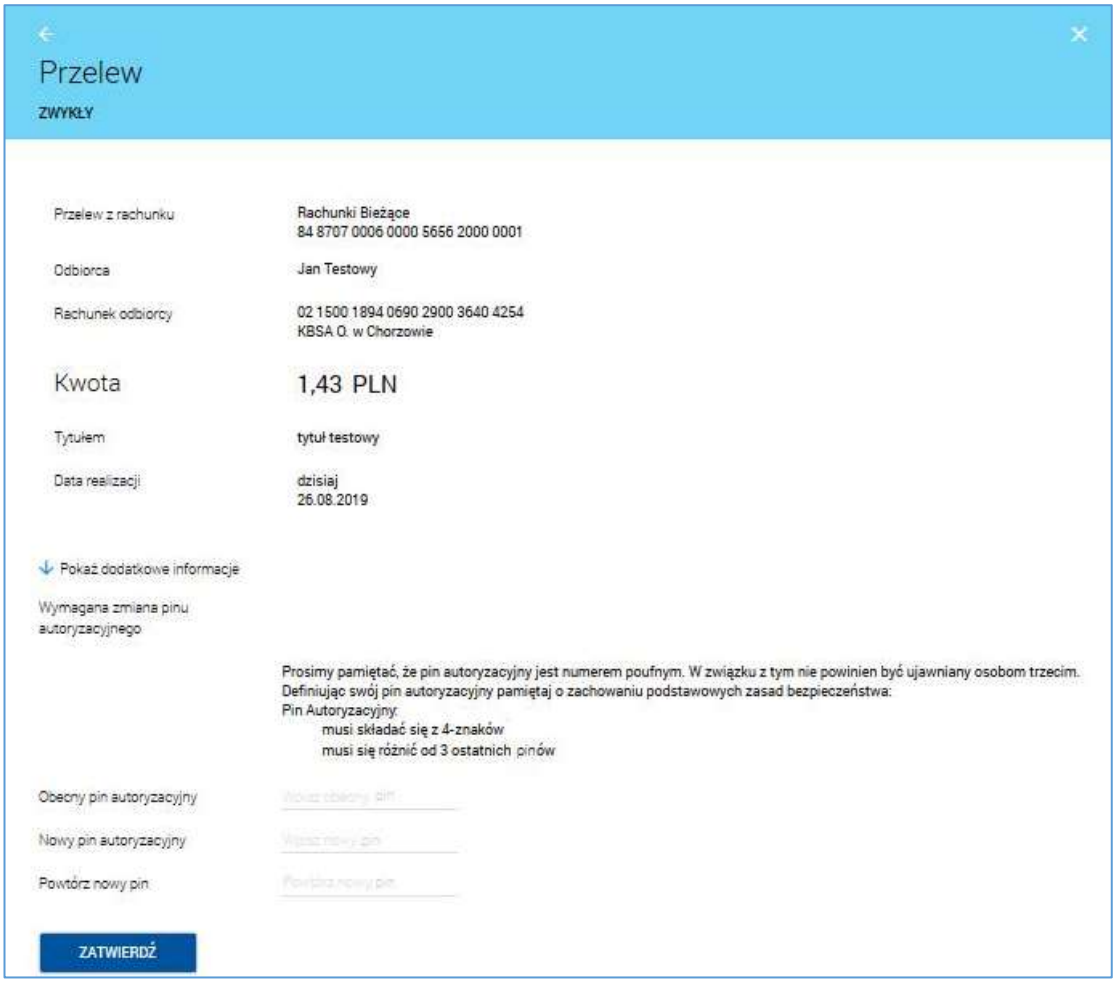


Wprowadzenie kodu SMS:

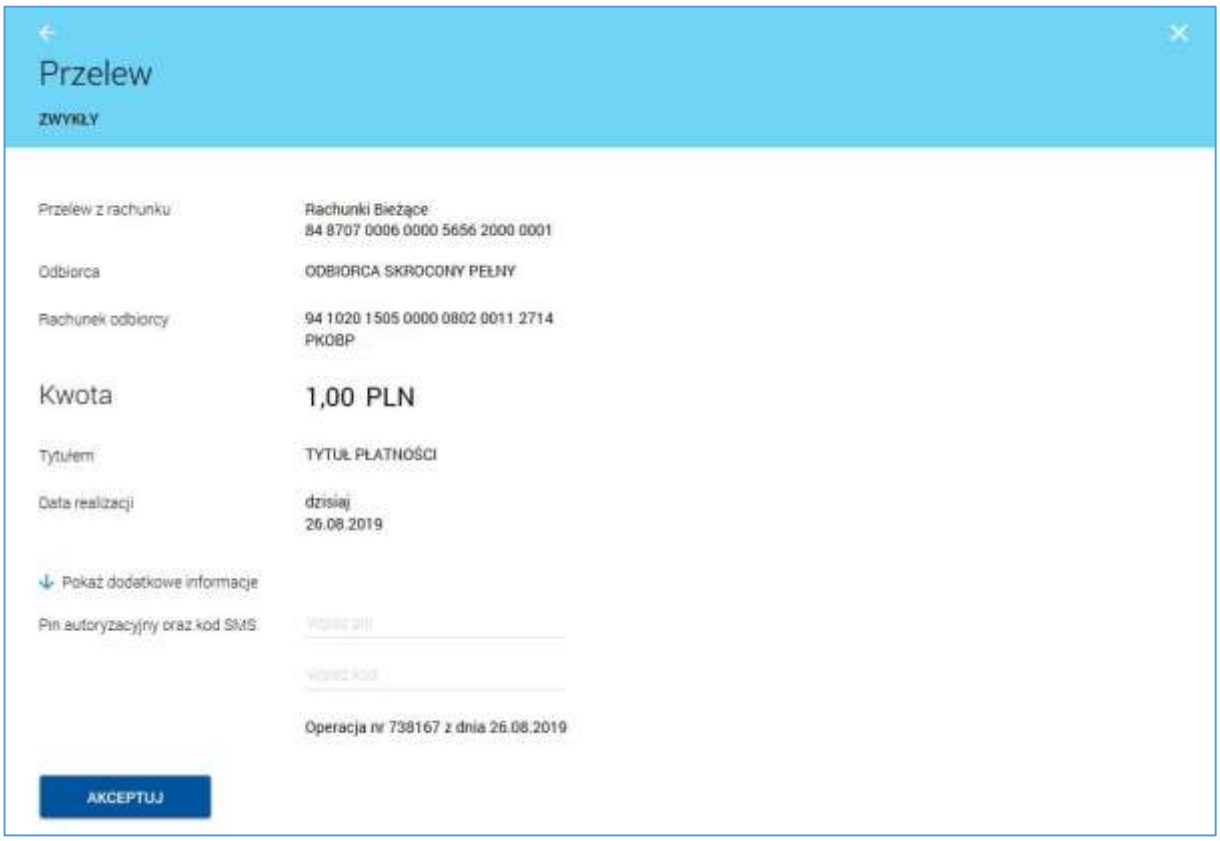


ii) autoryzacja:

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:



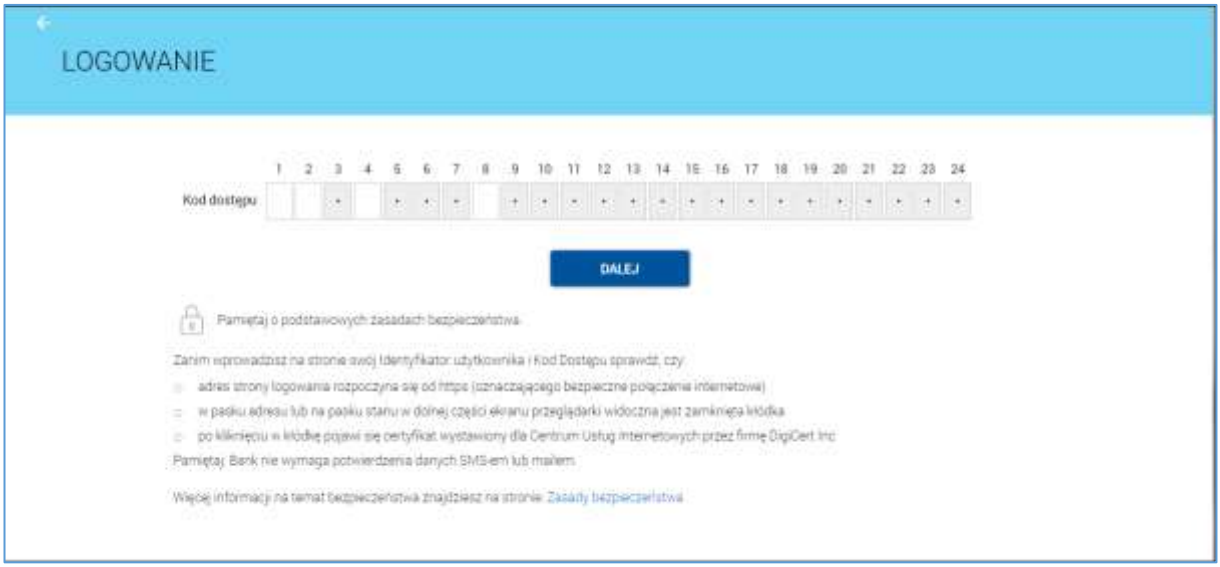
2.2. <u>Opis szczegółowy - schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Token mobilny Asseco MAA)</u>

a) Wygląd formatek dla użytkownika

i) autentykacja:

Wprowadzenie identyfikatora użytkownika:

Wprowadzenie hasła maskowanego:

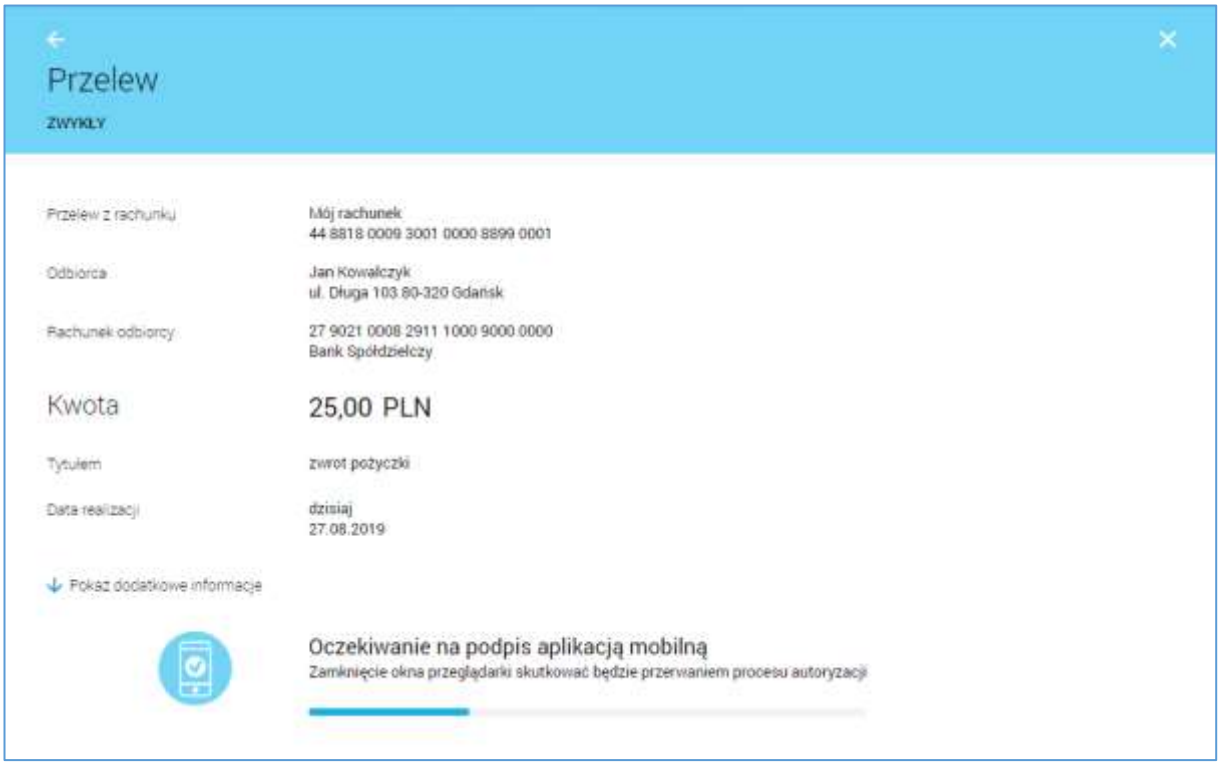


Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

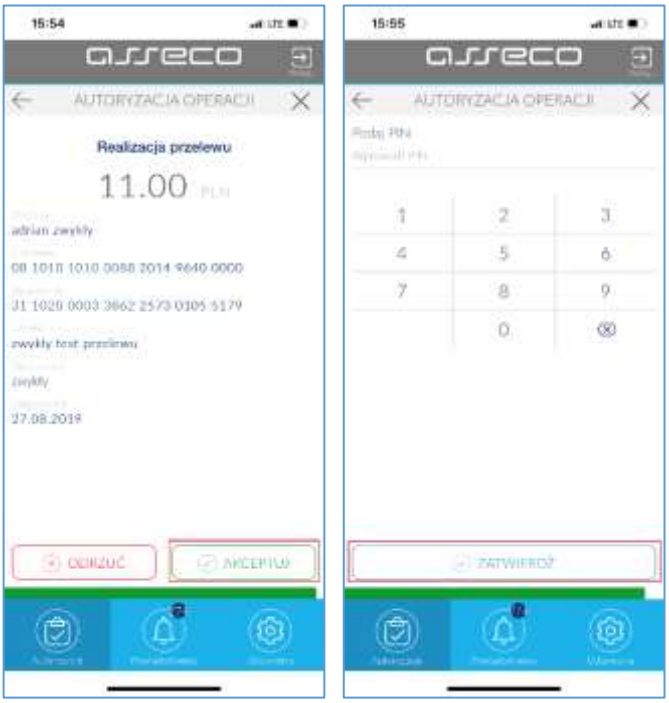
Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:

ii) autoryzacja:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:



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



2.3. <u>Opis szczegółowy – schemat nr 3 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe + Token RSA, autoryzacja: Hasło stałe + Token RSA)</u>

Zmiana metody autentykacji realizowana będzie w wariancie bez zmiany identyfikatora Klienta:

i) Pozyskanie numeru telefonu od Klienta

ii) Zmiana metody autentykacji na hasło maskowane.

iii) Przypisanie jednego ze środków dostępu:

- Autentykacja: hasło maskowane + kod SMS, autoryzacja: PIN + kod SMS
- Autentykacja: hasło maskowane + token mobilny Asseco MAA + PIN, autoryzacja: token mobilny Asseco MAA + PIN

iv) Przekazanie Klientowi hasła.