Bank Spółdzielczy
w Radzyniu Podlaskim

Dostosowanie środków dostępu użytkowanych w systemach bankowości elektronicznej Asseco CBP oraz def3000/CEB do wymagań SCA (silne uwierzytelnianie).

Spis treści:

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.:

a) Bankowość detaliczna – Asseco CBP
   - 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

b) Bankowość korporacyjna – def3000/CEB
   - autentykacja: hasło stałe, autoryzacja: karta mikroprocesorowa
   - autentykacja: hasło stałe + token RSA, autoryzacja: karta mikroprocesorowa

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[1]
2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN[2]	Token mobilny Asseco MAA + PIN[2]
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]
4	Hasło maskowane	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]

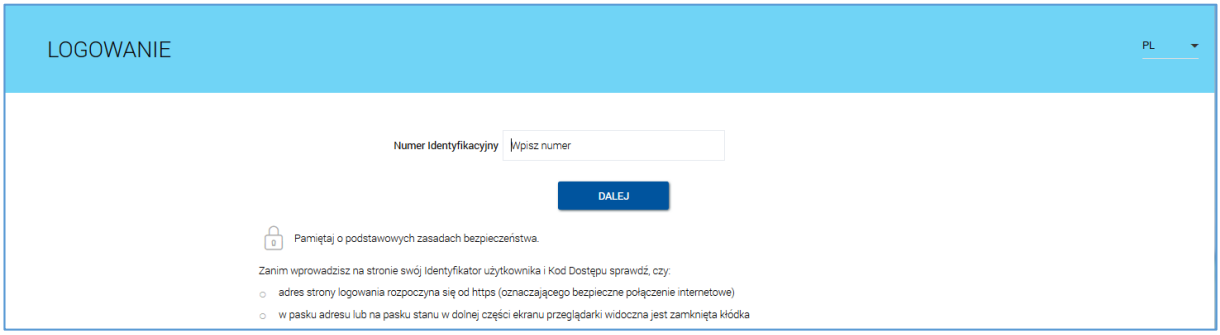
Legenda:
[1] - kod PIN autoryzujący. Klient zostanie poproszony o utworzenie PINu autoryzującego podczas pierwszej autoryzacji zlecenia.
[2] - kod PIN służący do logowania do aplikacji mToken mobilny Asseco MAA

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

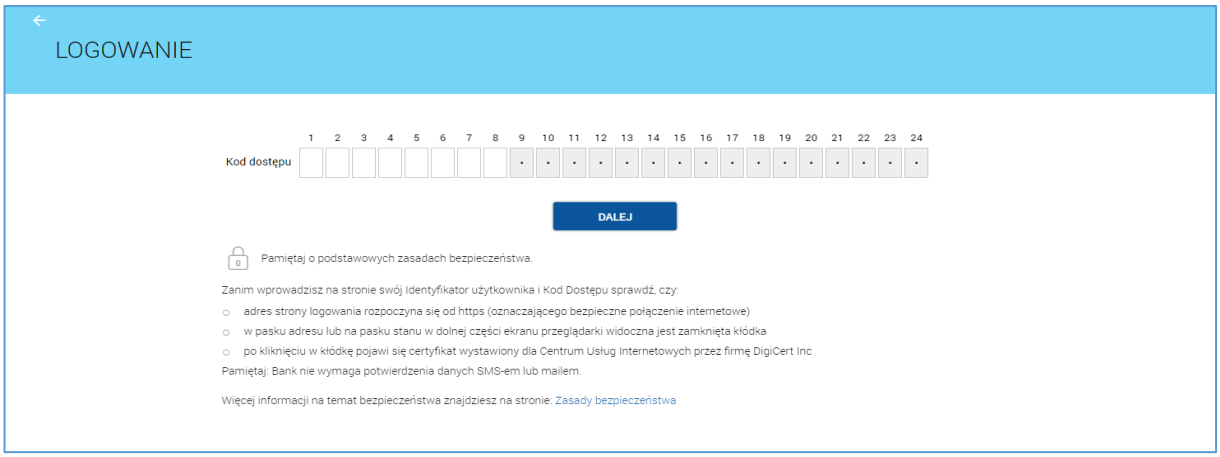
Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) autentykacja:

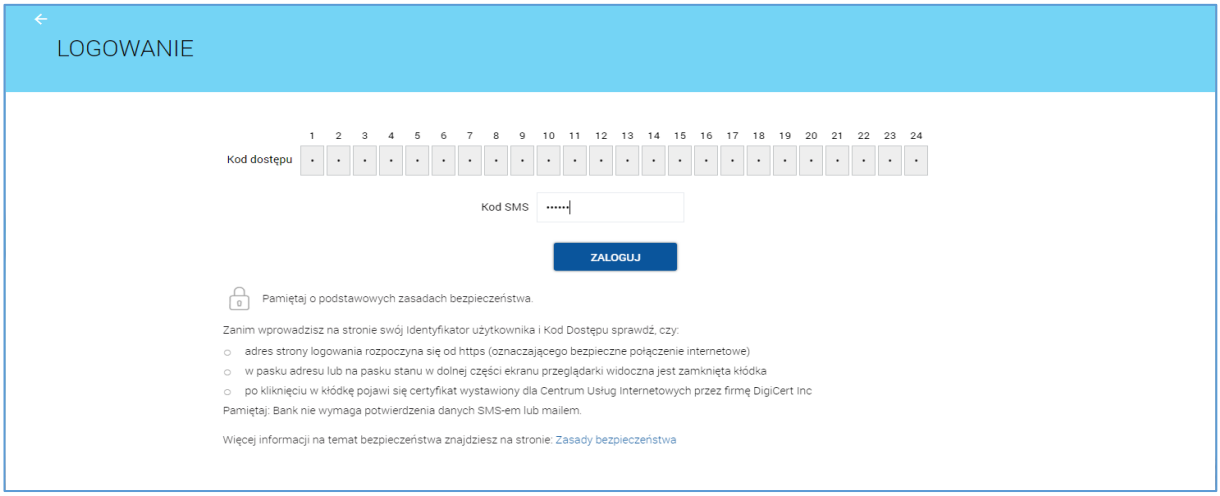
Wprowadzenie identyfikatora użytkownika:



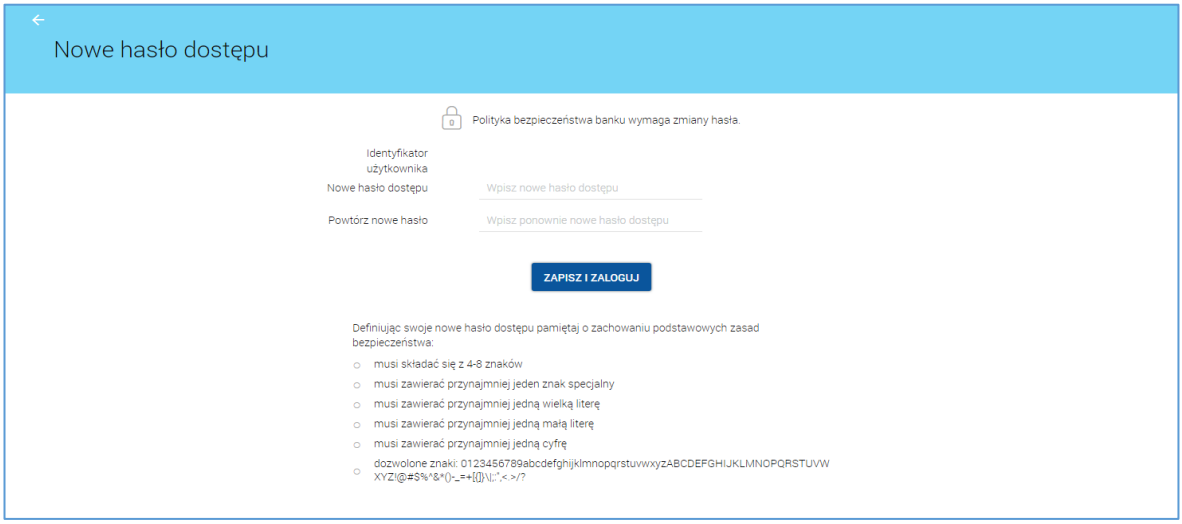
Wprowadzenie tymczasowego hasła, który klient otrzymał w wiadomości SMS:



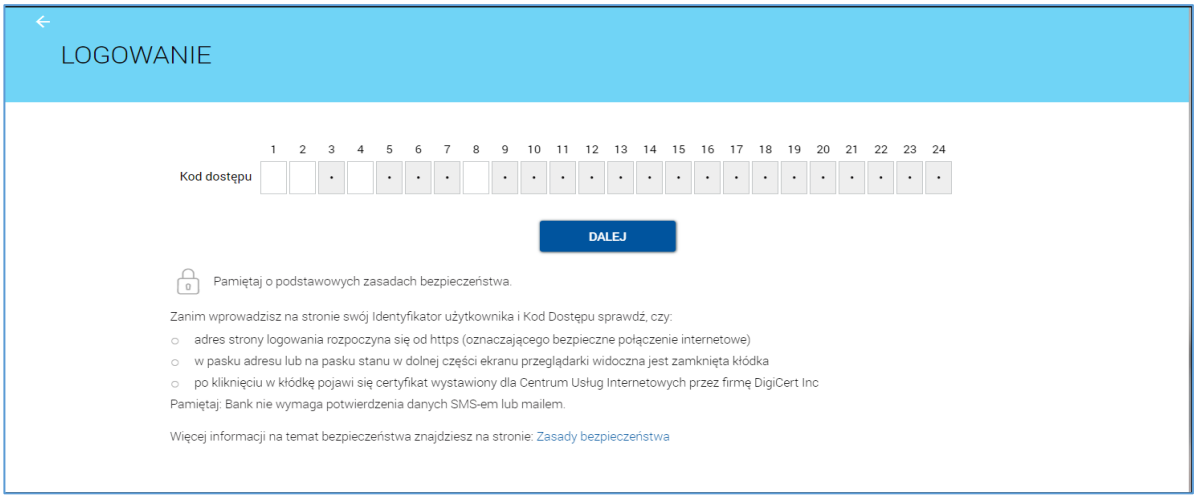
Zatwierdzanie tymczasowego hasła kodem SMS:



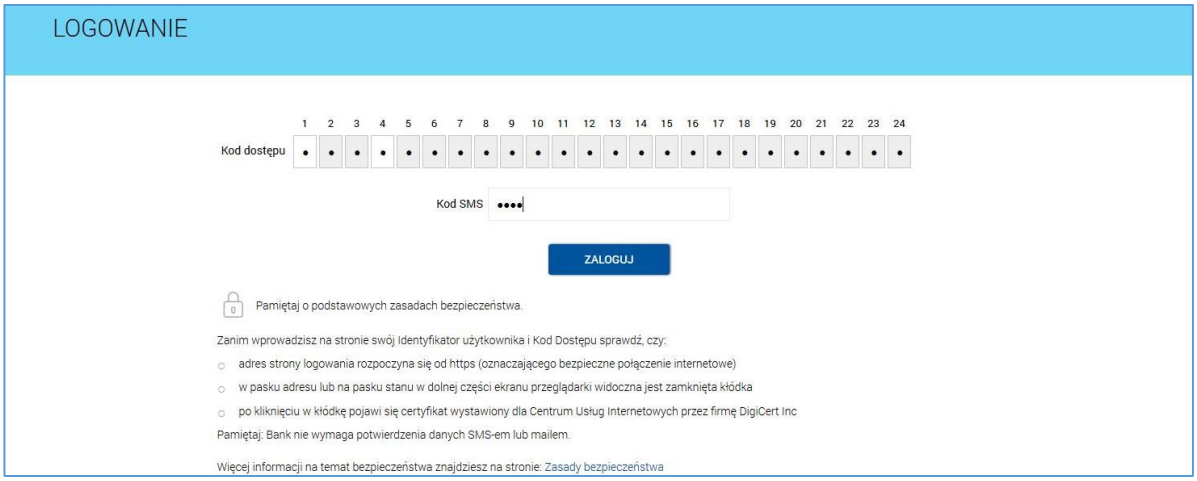
Ustalenie nowego hasła:



Ponowne logowanie do aplikacji z użyciem nowego hasła:

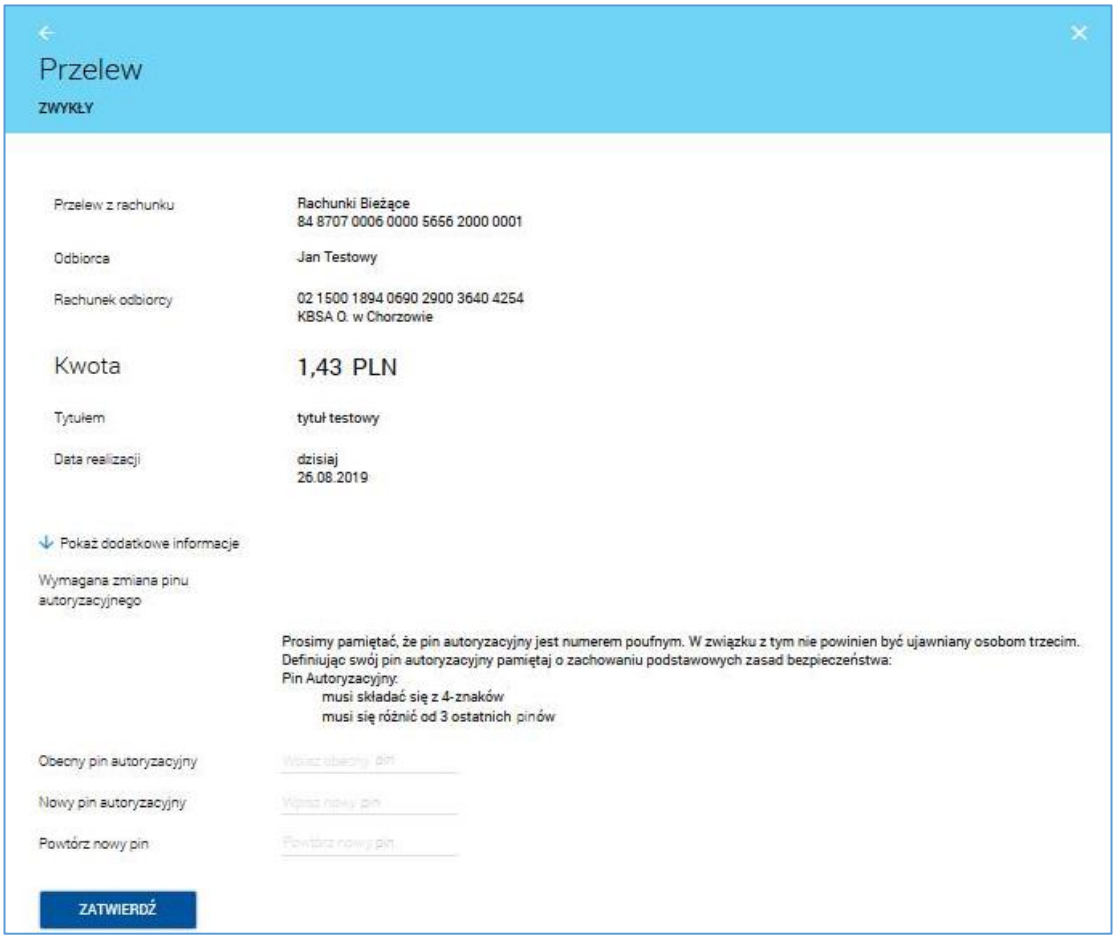


Wprowadzenie kodu SMS:

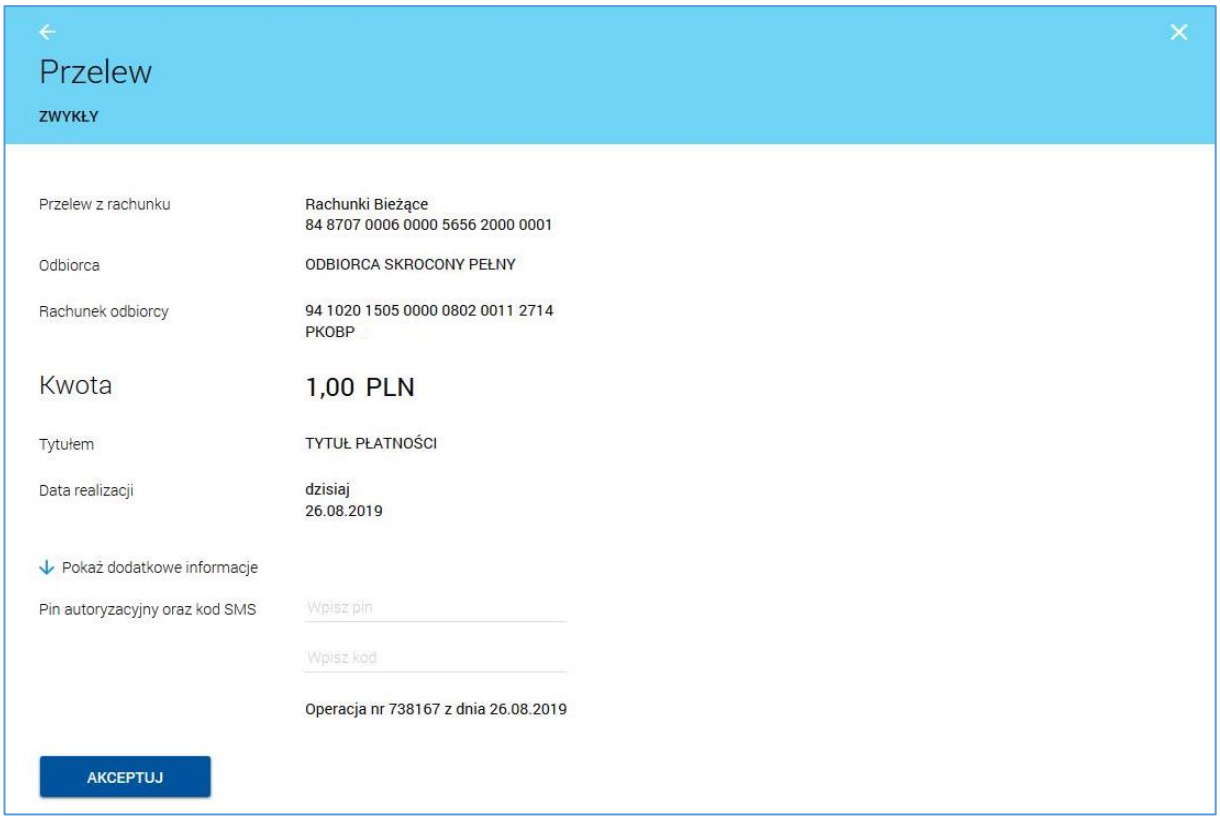


ii) autoryzacja:

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:

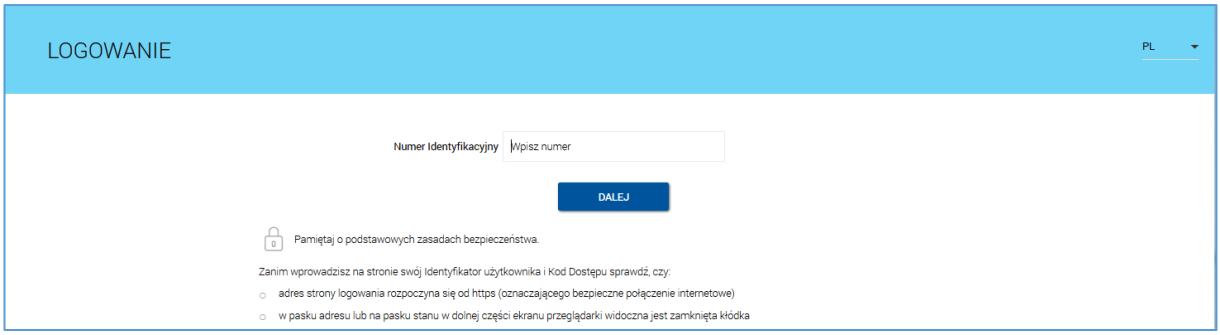


2.2. Opis szczegółowy - schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Token mobilny Asseco MAA)

Wygląd formatek dla użytkownika

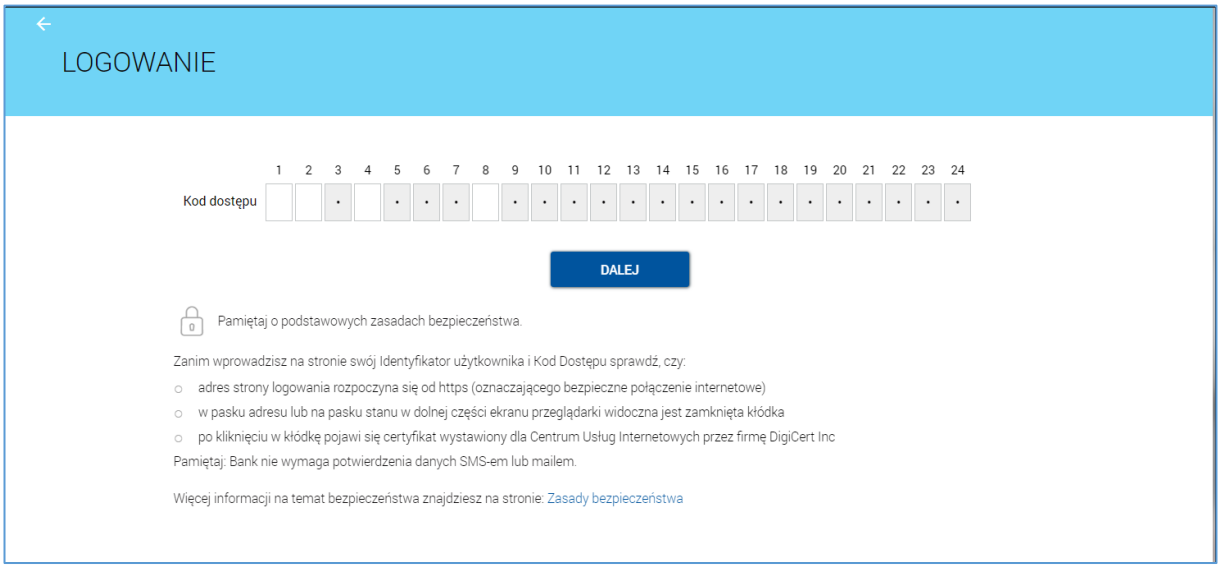
i) autentykacja:

Wprowadzenie identyfikatora użytkownika:

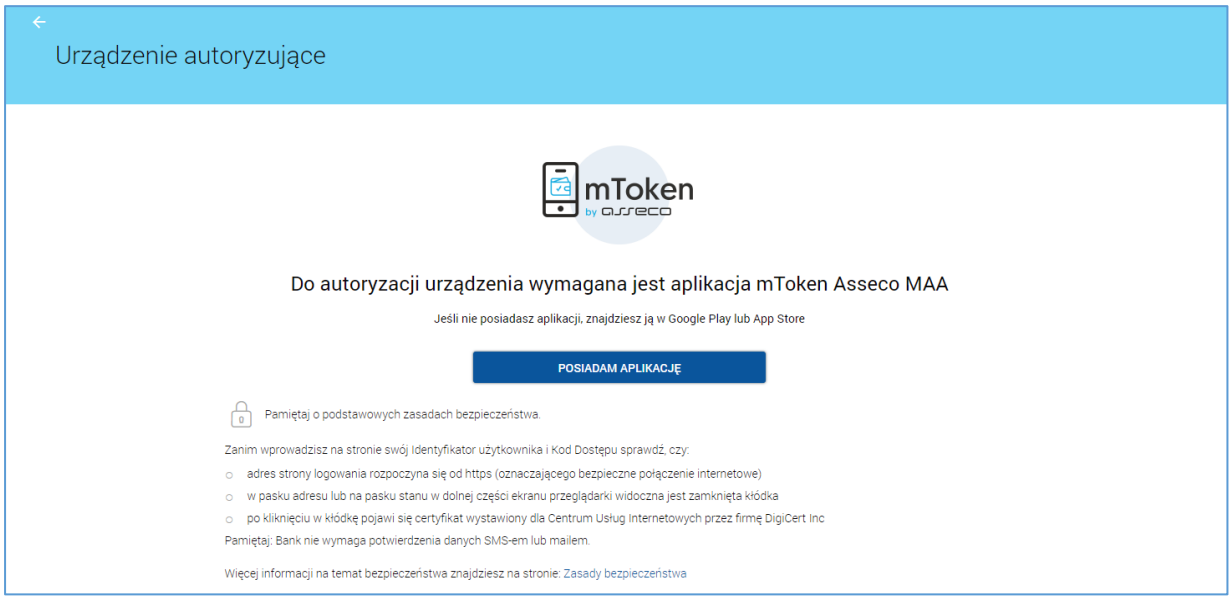


Wprowadzenie hasła maskowanego:

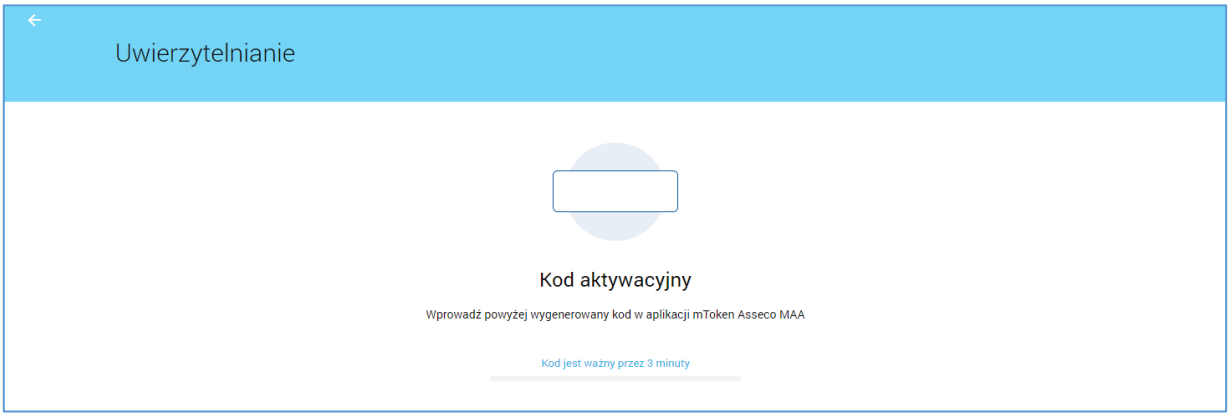
UWAGA! W przypadku pierwszego logowania, dla klienta, system w pierwszym kroku poprosi o podanie hasła startowego. Wówczas system najpierw poprosi o ustalenie nowego hasła a po ustaleniu nowego hasła, aplikacja wymusi ponowne logowanie już z nowym hasłem.



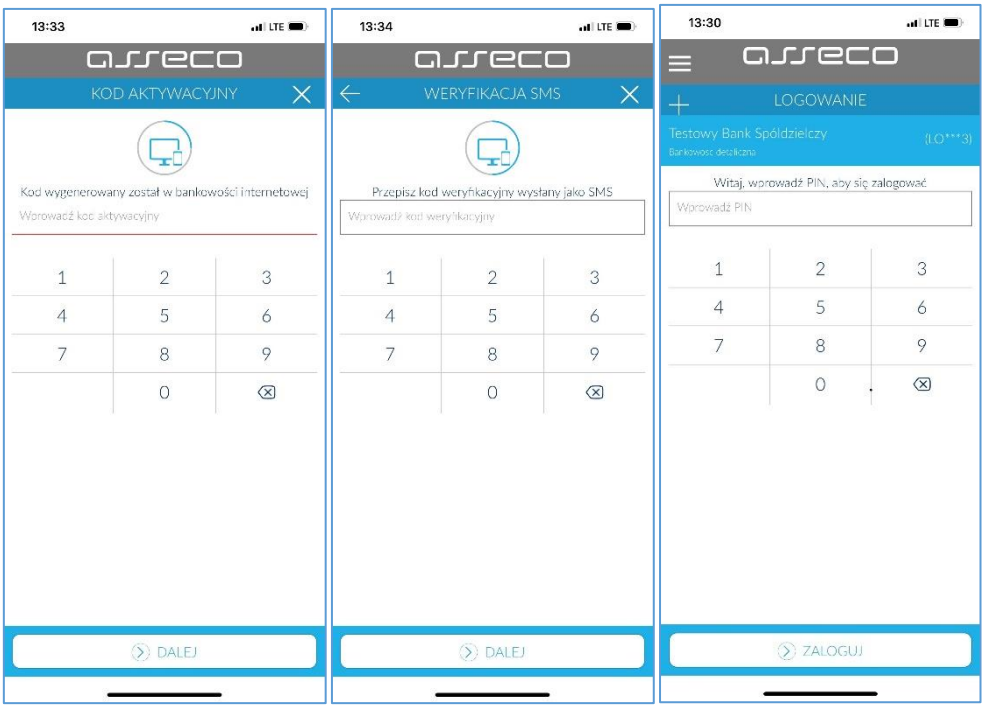
W przypadku braku sparowanego urządzenia, aplikacja wyświetli komunikat o sparowaniu urządzenia.



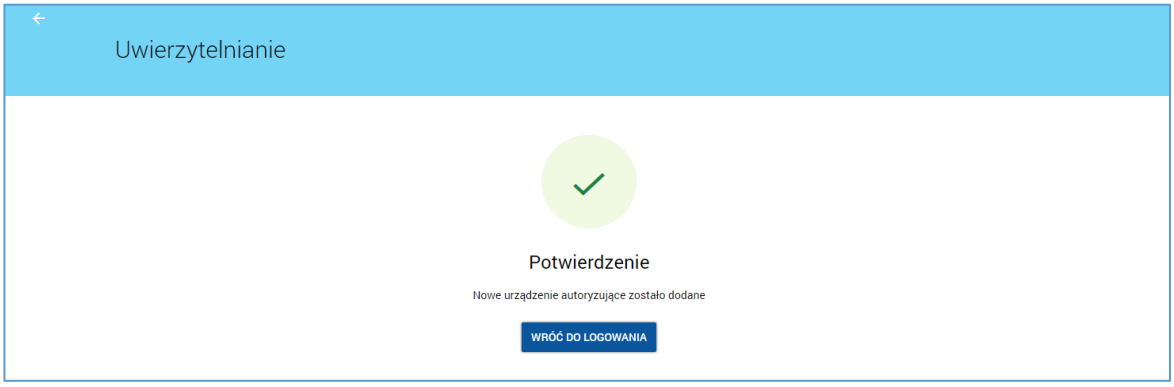
Po tym komunikacie, klient powinien pobrać aplikację na urządzenie mobilne. Po pobraniu aplikacji na urządzenie mobilne, w aplikacji internetowej Asseco CBP należy wybrać opcję „Posiadam aplikację”, gdzie wyświetla się kod aktywacyjny.



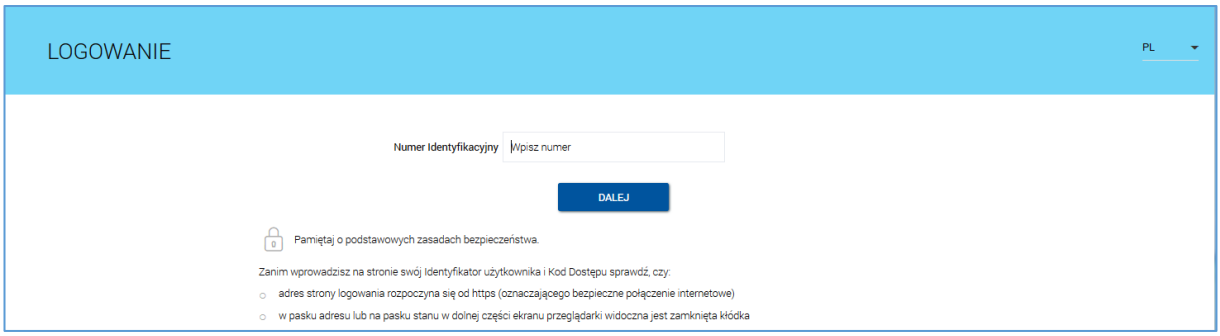
Na urządzeniu mobilnym klient, dodaje nowe urządzenie poprzez znak „+” i wprowadza kod, który wyświetli się w aplikacji internetowej (Kod w aplikacji Asseco CBP pokaże się po wejściu w opcję „Posiadam aplikację” (patrz zrzut powyżej)). W kolejnym kroku należy podać kod SMS, który zostanie przesłany na wskazany w Bank Admin numer telefonu i ustawić pin do aplikacji



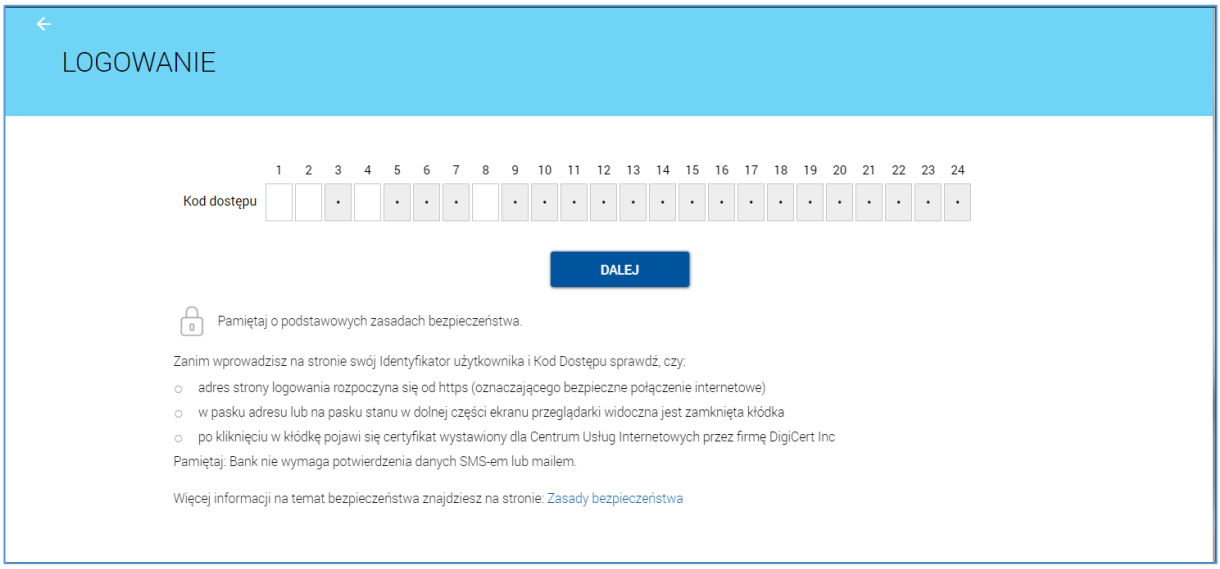
Po wykonaniu w/w czynności, w aplikacji pojawi się komunikat o poprawnym sparowaniu. I system poprosi o ponowne zalogowanie do bankowości.



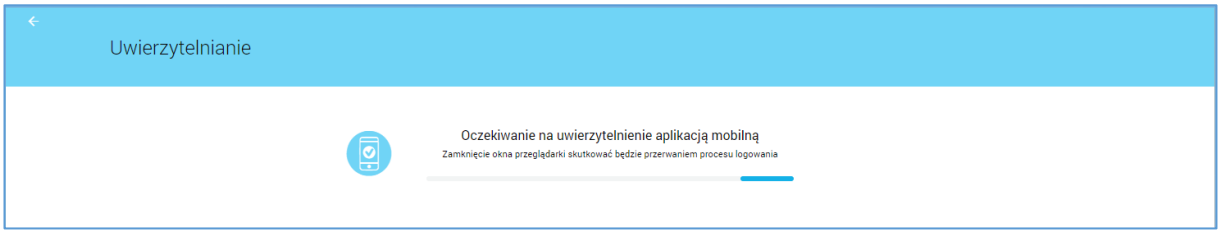
Wówczas ponownie należy wykonać akcję logowania: wprowadzenie identyfikatora użytkownika:



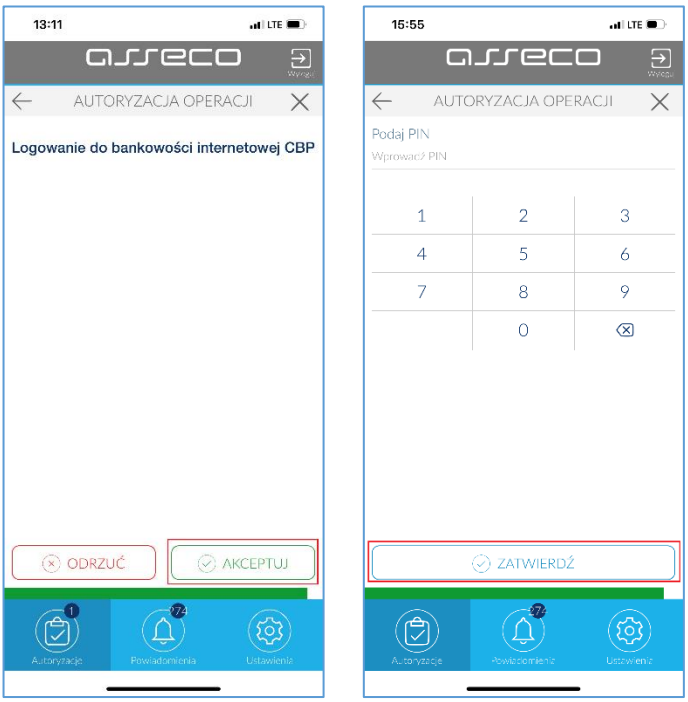
Wprowadzenie hasła maskowanego:



Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:



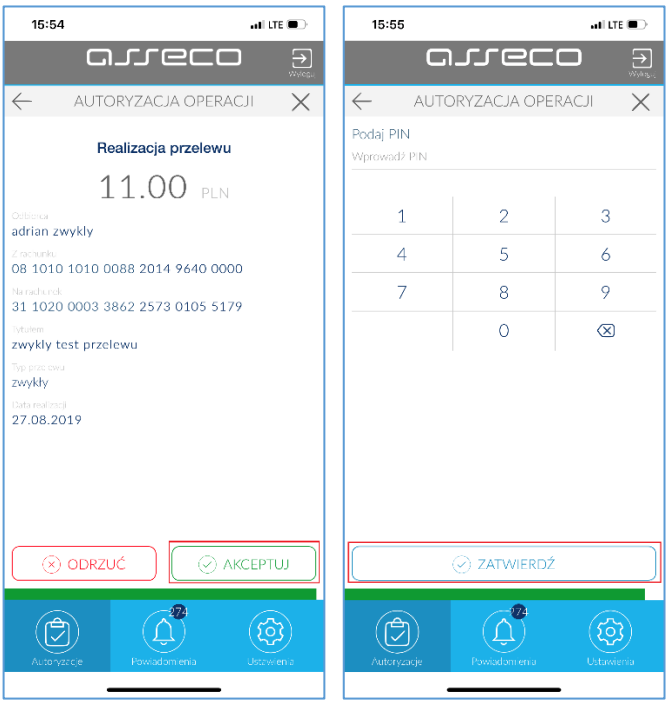
Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:



ii) autoryzacja:

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:

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



3. def3000/CEB – dostosowanie do wymagań SCA

Środki dostępu w bankowości korporacyjnej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w tabeli 2:

Tabela 2	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
Nr schematu „autentykacja - autoryzacja"	**Obecna autentykacja**	**Obecna autoryzacja**	**Nowa autentykacja**	**Nowa autoryzacja**
1	Hasło stałe	Karta mikroprocesorowa (aplet java) + PIN	Karta mikroprocesorowa (aplet java) + PIN[1]	Karta mikroprocesorowa (aplet java) + PIN[1]
2	Hasło stałe + token RSA	Karta mikroprocesorowa (aplet java) + PIN	Hasło stałe + token RSA	Karta mikroprocesorowa (aplet java) + PIN[1]

Legenda:
[1] - PIN do karty mikroprocesorowej
[2] - PIN służący do uruchomienia tokena VASCO
[3] - PIN do karty mikroprocesorowej wpisywany w aplikacji SCSA
[4] - PIN służący do uruchomienia aplikacji mToken Asseco MAA

3.1. Opis szczegółowy schemat nr 1 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe, autoryzacja: Karta mikroprocesorowa (aplet java) + PIN)

a) Zmiana sposobu logowania (z hasła stałego na autentykację kartą mikroprocesorową) zostanie wprowadzona dla wszystkich użytkowników w jednym terminie przez Asseco Poland S.A.

UWAGA:
W celu dostosowania systemu do wymogów SCA konieczne jest wyłączenia logowania samym hasłem stałym. Zatem po dniu 2019-09-13 użytkownik posługujący się tą metodą autentykacji (np. użytkownik pasywny bez środka autoryzacji) straci dostęp do def3000/CEB do momentu wydania mu środka autentykacji zgodnego z SCA.

b) Wygląd formatek dla użytkownika

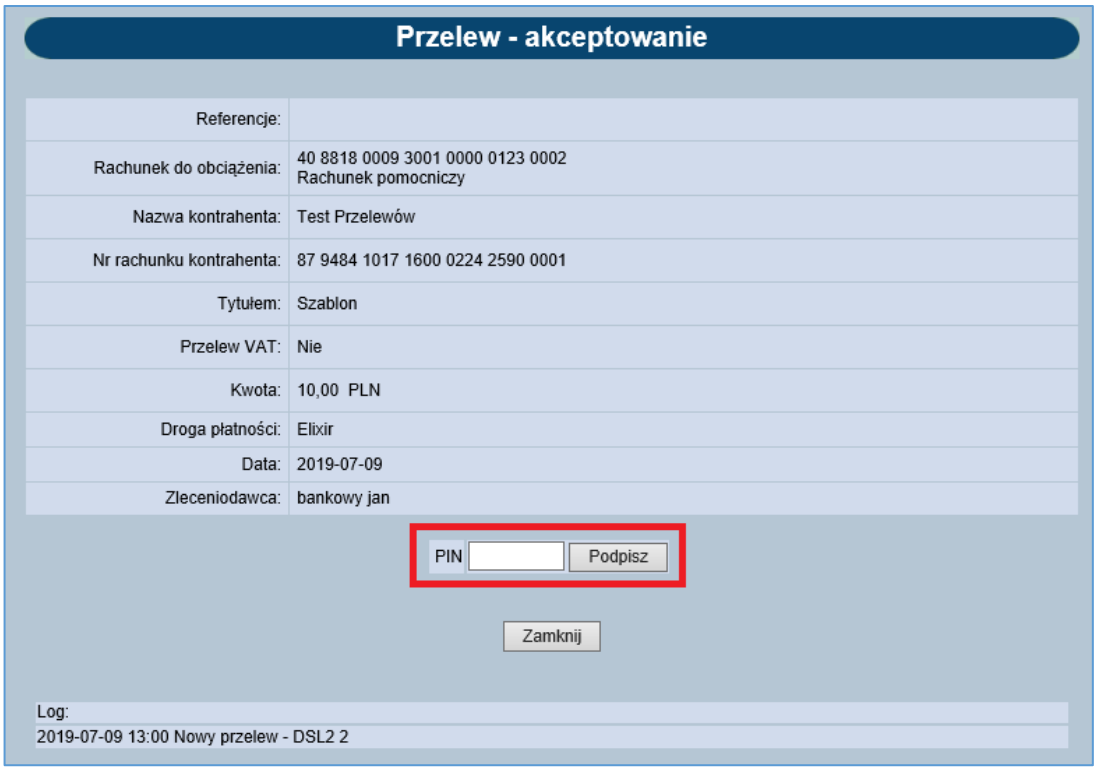
i) autentykacja:

Wybór metody autentykacji – Logowanie karta mikroprocesorową:

Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:

ii) autoryzacja:

Umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:



3.2. Opis szczegółowy – schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe + token RSA, autoryzacja: Karta mikroprocesorowa (aplet java) +PIN)

a) Rekonfiguracja użytkowników nie jest wymagana.

b) Wygląd formatek dla użytkownika pozostaje bez zmian.