Bank Spółdzielczy
w Dołhobyczowie

Dostosowanie środków dostępu użytkowanych w systemach bankowości elektronicznej korporacyjnej def3000/CEB do 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 korporacyjna – def3000/CEB</u>

- autentykacja: hasło stałe, autoryzacja: karta mikroprocesorowa
- autentykacja: token VASCO DP 260, autoryzacja: token VASCO DP 260

2. def3000/CEB – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej 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	Karta mikroprocesorowa (aplet java) + PIN
2	Hasło stałe + token VASCO DP260	Token VASCO DP260 + PIN	Hasło stałe + token VASCO DP260 + PIN	Karta mikroprocesorowa (aplikacja SCSA) + PIN

2.1. 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.

b) Wygląd formatek dla użytkownika

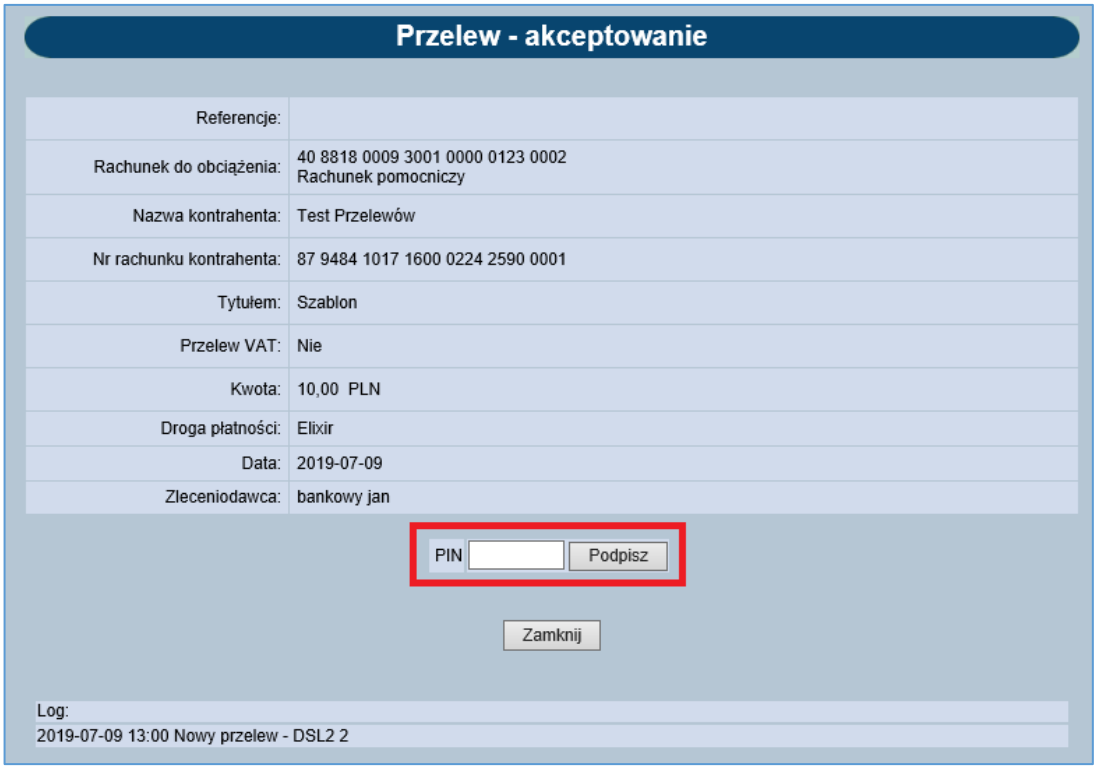
i) autentykacja:

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:



2.2. <u>Opis szczegółowy – schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe + token VASCO DP260, autoryzacja: Token VASCO DP260+PIN)</u>

a) Wydanie nowego środka dostępu do autoryzacji
Bank wykona rekonfigurację użytkownika:

- Autoryzacja: aplikacja SCSA (karta mikroprocesorowa z obsługą SCSA + PIN)

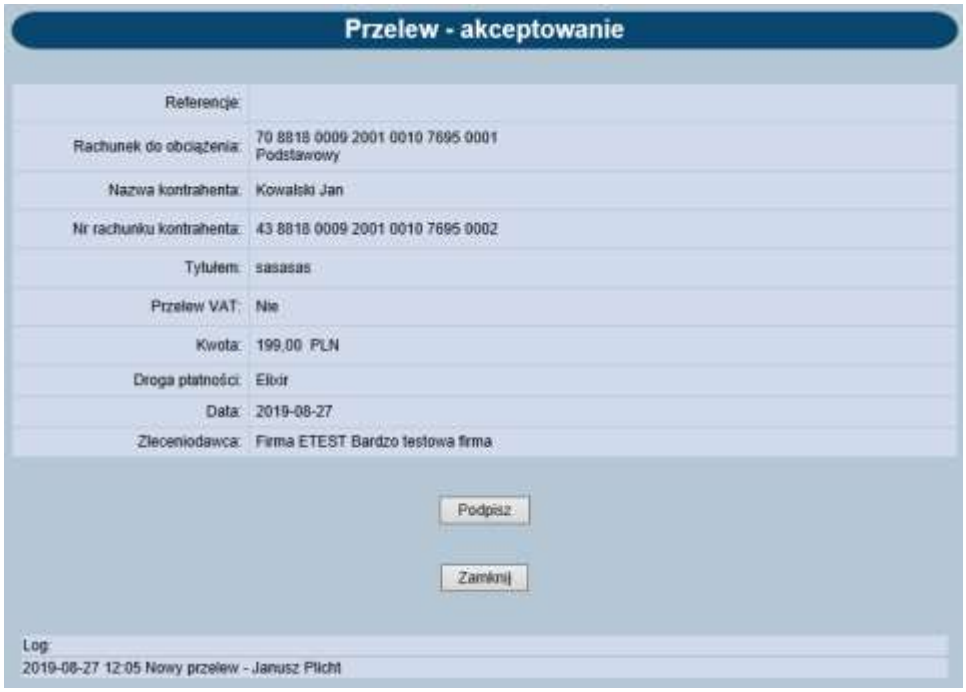
b) Wygląd formatek dla użytkownika

i) autentykacja token VASCO DP260:

Wybór metody autentykacji – Logowanie tokenem VASCO:

ii) autoryzacja kartą mikroprocesorową z aplikacją SCSA:

Zlecenie do autoryzacji:



Autoryzacja zlecenia w aplikacji SCSA (wymagane jest umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:

Potwierdzenie autoryzacji: