

## **Dostosowanie środków dostępu użytkowanych w CUI/CBP do wymogów silnego uwierzytelniania (SCA).**

Ze względu na wymogi dyrektywy unijnej PSD2 (Payment Services Directive 2), Bank Spółdzielczy w Świdnicy wprowadza zmiany w korzystaniu z bankowości elektronicznej. Zmiany te pozwolą jeszcze lepiej zabezpieczyć dostęp do Państwa finansów.

Obecnie stosowane środki dostępu do systemu bankowości elektronicznej CUI/CBP 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 np. dane biometryczne), 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 i zostanie zaimplementowana w systemie CUI/CBP w dniach od 2019-09-11 do dnia 2019-09-13.

Poniżej prezentujemy opis możliwych do wyboru w systemie CUI/CBP rozwiązań dotyczących logowania i autoryzacji.

## Logowanie i autoryzacja - schemat nr 1 (logowanie: hasło maskowane + kod SMS, autoryzacja: kod SMS + PIN)


### Logowanie: hasło maskowane + kod SMS

Po wpisaniu w przeglądarce internetowej adresu strony do logowania do systemu CUI/CBP (<https://cbp.cui.pl>), wyświetlane jest okno logowania.

# LOGOWANIE

Numer Identyfikacyjny

[DALEJ](#)

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka

Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator użytkownika i użyć przycisku [DALEJ].

Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami. Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia kodu dostępu (hasła maskowanego).

## LOGOWANIE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Kod dostępu	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

DALEJ



Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

W polu Kod dostępu należy w losowo wybrane puste pola wprowadzić wymagane pozycje z hasła (własne hasło utworzone wcześniej przez użytkownika). Pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola do uzupełnienia. Na przykład, jeżeli pole 1 jest puste, to należy wprowadzić pierwszy znak ze swojego hasła. Jeżeli pole 2 jest puste, należy wprowadzić drugi znak ze swojego hasła itd. Po wprowadzeniu poprawnego kodu dostępu należy użyć przycisku [DALEJ].

Wyświetlone zostanie okno służące do wprowadzenia kodu SMS, wysłanego na przypisany do Klienta numer telefonu. Kod otrzymany w wiadomości SMS należy wpisać w odpowiednim polu.

## LOGOWANIE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Kod dostępu	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Kod SMS

ZALOGUJ



Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Jeżeli wszystkie dane w procesie autentykacji zostały wprowadzone prawidłowo, po naciśnięciu przycisku [ZALOGUJ] udostępniony zostanie system bankowości internetowej CUI/CBP.

## Autoryzacja: kod SMS + PIN

Pierwsza autoryzacja poprzedzona jest wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany.

### Przelew

ZWYKŁY

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	Jan Testowy
Rachunek odbiorcy	02 1500 1894 0690 2930 3640 4254 KBSA O. w Chorzowie
<b>Kwota</b>	<b>1,43 PLN</b>
Tytułem	tytuł testowy
Data realizacji	dzisiaj 26.08.2019

↓ Pokaż dodatkowe informacje

Wymagana zmiana pinu autoryzacyjnego

Prosimy pamiętać, że pin autoryzacyjny jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swój pin autoryzacyjny pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

Pin Autoryzacyjny:  
musi składać się z 4-znaków  
musi się różnić od 3 ostatnich pinów

Obecny pin autoryzacyjny	<input type="text" value="Wpisz obecny pin"/>
Nowy pin autoryzacyjny	<input type="text" value="Wpisz nowy pin"/>
Powtórz nowy pin	<input type="text" value="Powtórz nowy pin"/>

**ZATWIERDŹ**

Kolejne autoryzacje wymagają wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS.

←

# Przelew

ZWYKŁY

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	ODBIORCA SKROCONY PEŁNY
Rachunek odbiorcy	94 1020 1505 0000 0802 0011 2714 PKOBP
<b>Kwota</b>	<b>1,00 PLN</b>
Tytułem	TYTUŁ PŁATNOŚCI
Data realizacji	dzisiaj 26.08.2019
↓ Pokaż dodatkowe informacje	
Pin autoryzacyjny oraz kod SMS	<input type="text" value="Wpisz pin"/>
	<input type="text" value="Wpisz kod"/>
	Operacja nr 738167 z dnia 26.08.2019

**AKCEPTUJ**

## Logowanie i autoryzacja - schemat nr 2 (logowanie: hasło maskowane + token mobilny Asseco MAA + PIN, autoryzacja: token mobilny Asseco MAA + PIN)

### Logowanie: hasło maskowane + token mobilny Asseco MAA + PIN

Po wpisaniu w przeglądarce internetowej adresu strony do logowania do systemu CUI/CBP (<https://cbp.cui.pl>), wyświetlane jest okno logowania.

# LOGOWANIE

Numer Identyfikacyjny

DALEJ



Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka

Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator użytkownika i użyć przycisku [DALEJ].

Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji rozpatruje tę wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami. Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia kodu dostępu (hasła maskowanego).

## LOGOWANIE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Kod dostępu	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

DALEJ



Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- o w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- o po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

W polu Kod dostępu należy w losowo wybrane puste pola wprowadzić wymagane pozycje z hasła (własne hasło utworzone wcześniej przez użytkownika). Pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola do uzupełnienia. Na przykład, jeżeli pole 1 jest puste, to należy wprowadzić pierwszy znak ze swojego hasła. Jeżeli pole 2 jest puste, należy wprowadzić drugi znak ze swojego hasła itd. Po wprowadzeniu poprawnego kodu dostępu należy użyć przycisku [DALEJ].

Pojawi się okno z informacją o oczekiwaniu na uwierzytelnienie aplikacją mobilną.

## Uwierzytelnianie



### Oczekiwanie na uwierzytelnienie aplikacją mobilną

Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania

W tym momencie na urządzeniu mobilnym (telefon, tablet) należy zalogować się do aplikacji mToken Asseco MAA, zatwierdzić przyciskiem „Akceptuj” operację logowania do bankowości internetowej, następnie wprowadzić PIN aplikacji mobilnej i potwierdzić przyciskiem „Zatwierdź”.



### Logowanie do bankowości internetowej CBP



Podaj PIN

Wprowadź PIN

1	2	3
4	5	6
7	8	9
	0	✕



Jeżeli wszystkie dane w procesie autentykacji zostały wprowadzone prawidłowo, po zatwierdzeniu w aplikacji mToken Asseco MAA operacji logowania, nastąpi przekierowanie do systemu bankowości internetowej CUI/CBP.



## Autoryzacja: token mobilny Asseco MAA + PIN

Przy autoryzacji operacji pojawi się informacja o oczekiwaniu na podpis aplikacją mobilną.

### Przelew

ZWYKŁY

Przelew z rachunku	Mój rachunek 44 8818 0009 3001 0000 8899 0001
Odbiorca	Jan Kowalczyk ul. Długa 103 80-320 Gdańsk
Rachunek odbiorcy	27 9021 0008 2911 1000 9000 0000 Bank Spółdzielczy
Kwota	25,00 PLN
Tytułem	zwrot pożyczki
Data realizacji	dzisiaj 27.08.2019

↓ Pokaż dodatkowe informacje



#### Oczekiwanie na podpis aplikacją mobilną

Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu autoryzacji

W tym momencie na urządzeniu mobilnym (telefon, tablet) należy zalogować się do aplikacji mToken Asseco MAA, zatwierdzić przyciskiem „Akceptuj” operację , następnie wprowadzić PIN aplikacji mobilnej i potwierdzić przyciskiem „Zatwierdź”.

