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.

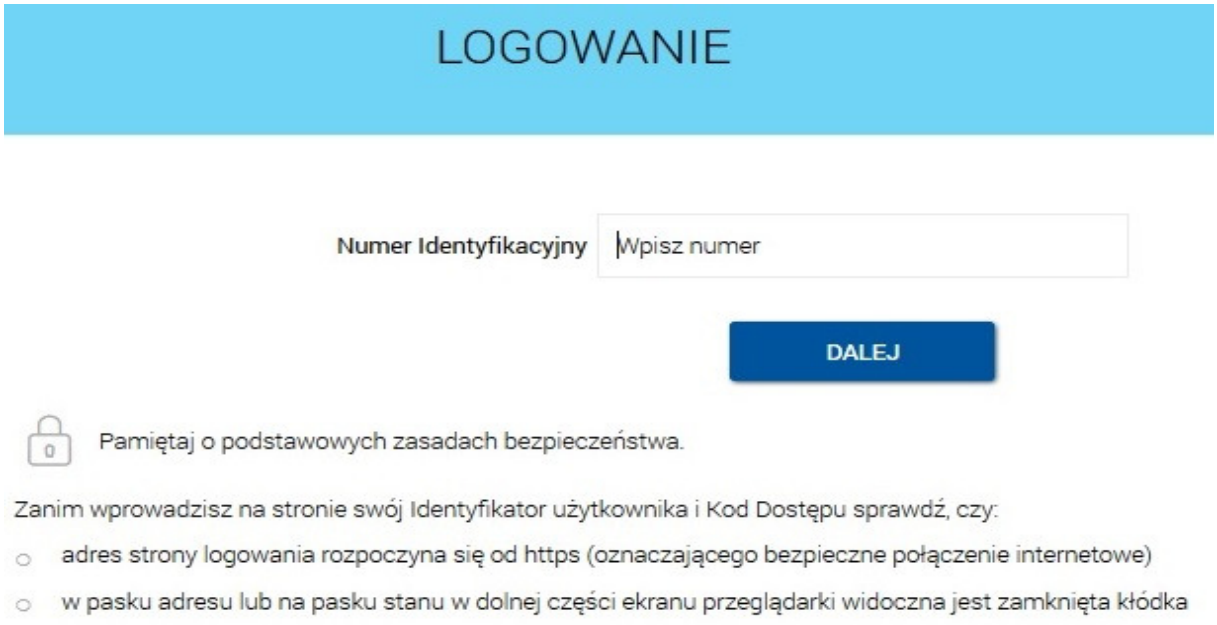
Dostosowanie do wymogów SCA dotyczy procesu autentykacji (logowania) oraz autoryzacji (podpisu). W/w zasada (SCA) determinuje zmiany w obecnie użytkowanych schematach środków dostępu i zostanie zaimplementowana w systemie CUI/CBP w dniach od 2019-09-11 do dnia 2019-09-13.

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.

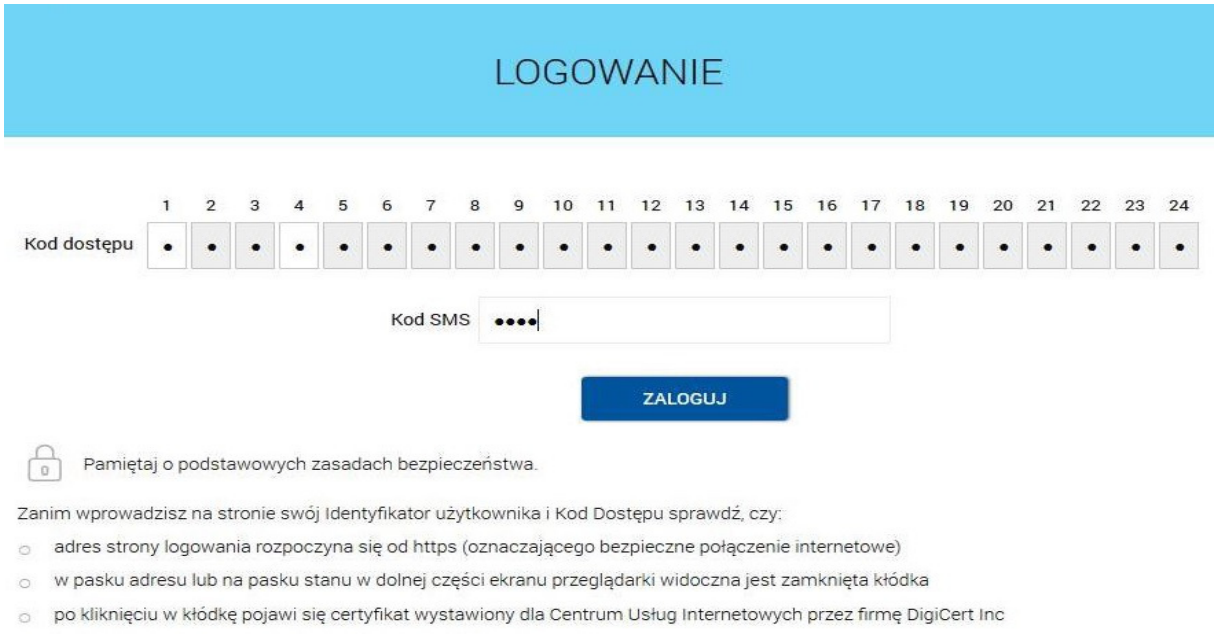


Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator użytkownika i użyć przycisku [DALEJ].

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).

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].

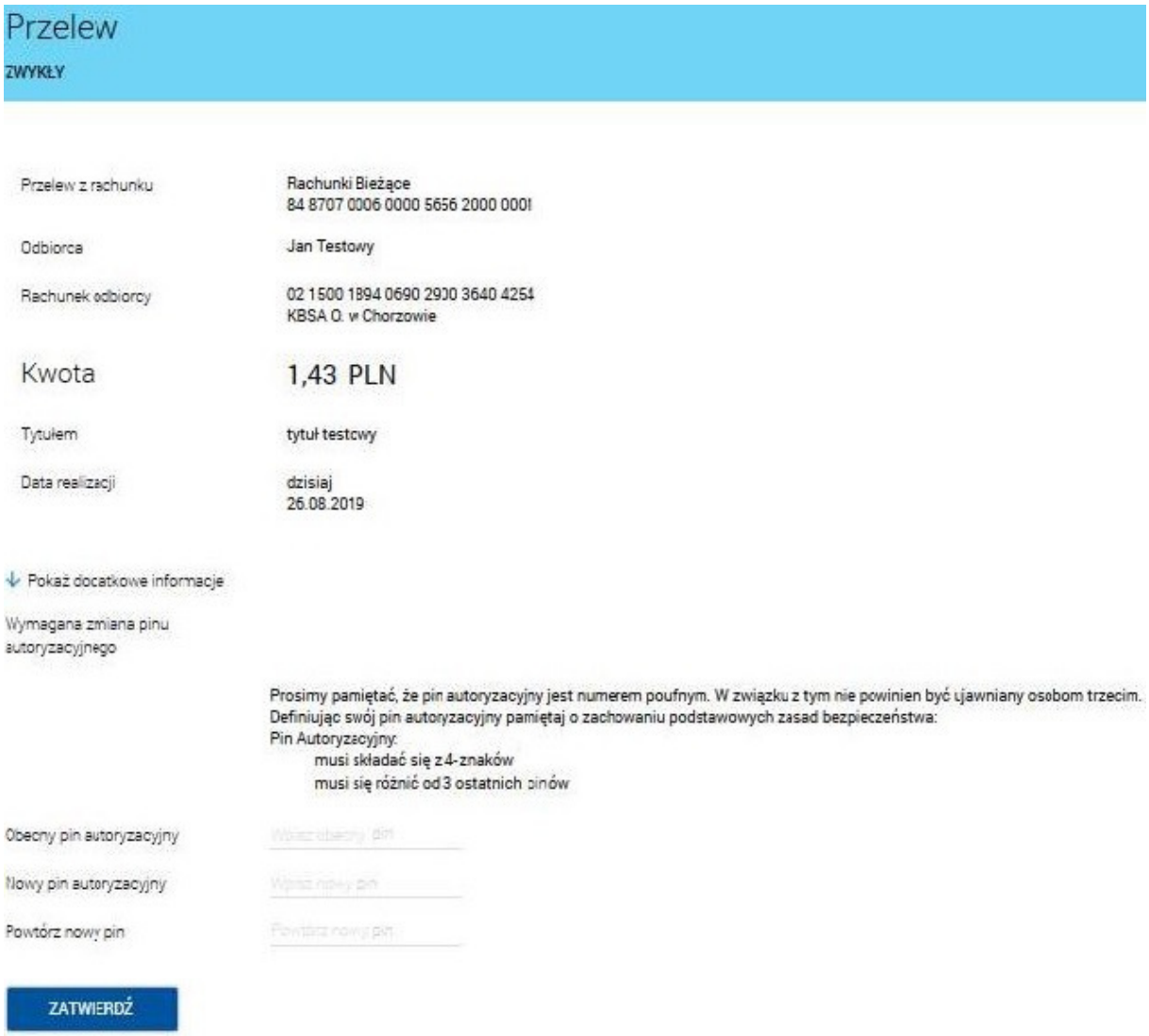
Wyświetlone zostanie okno służące do wprowadzenia kodu SMS, wysyłanego na przypisany do Klienta numer telefonu. Kod otrzymany w wiadomości SMS należy wpisać w odpowiednim polu.



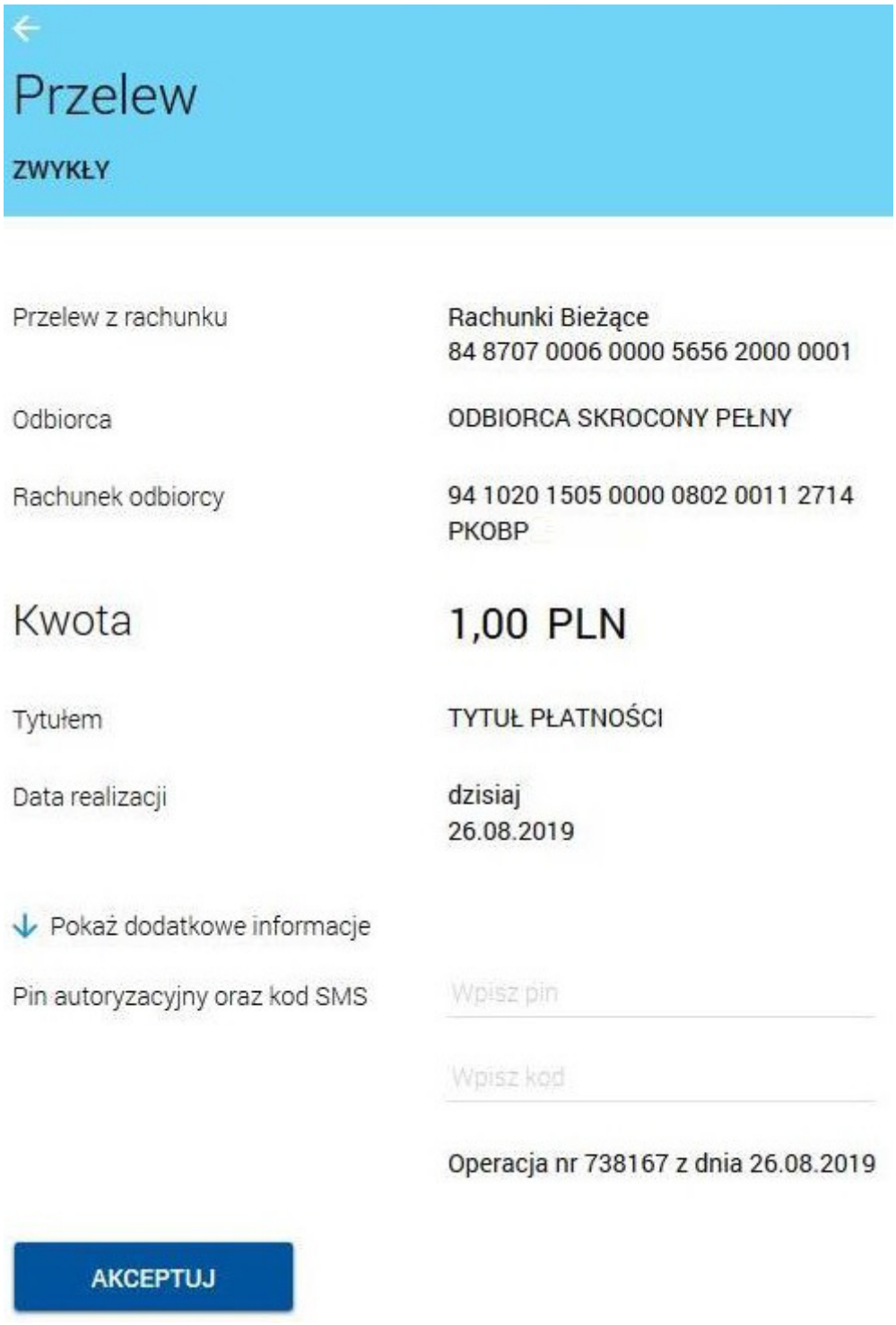
Jeżeli wszystkie dane w procesie autentykacji zostały wprowadzone prawidłowo, po naciśnięciu przycisku [ZALOGUJ] udostępniony zostanie system bankowości internetowej CUI/CBP.

Autoryzacja: kod SMS + PIN

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



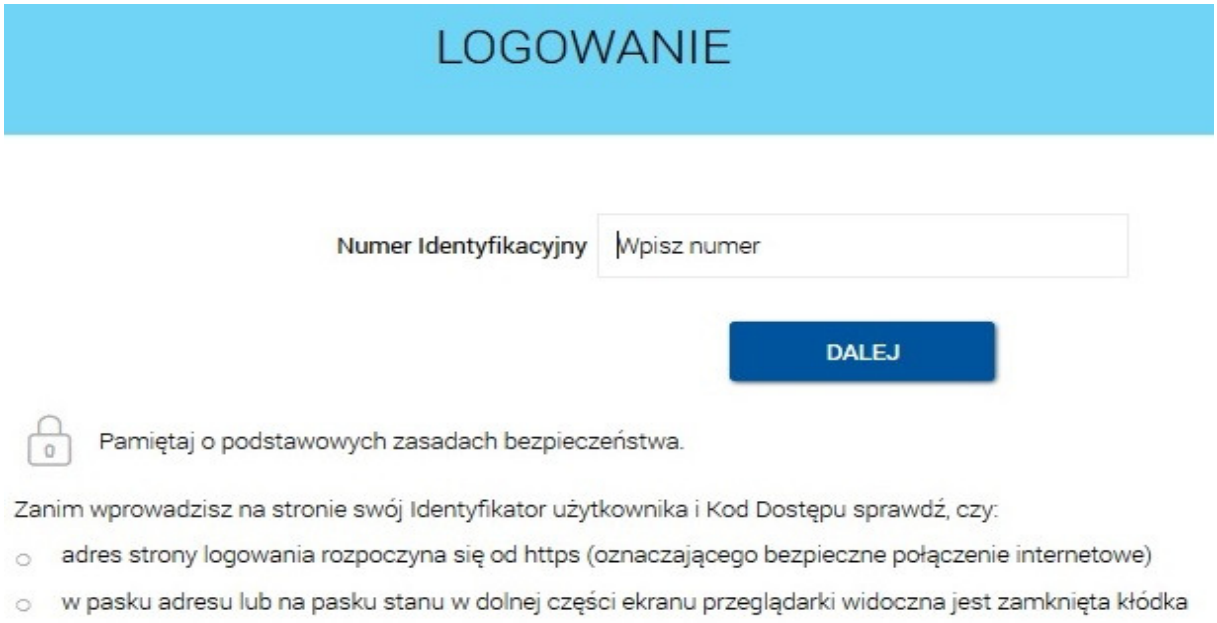
Kolejne autoryzacje wymagają wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS.



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.

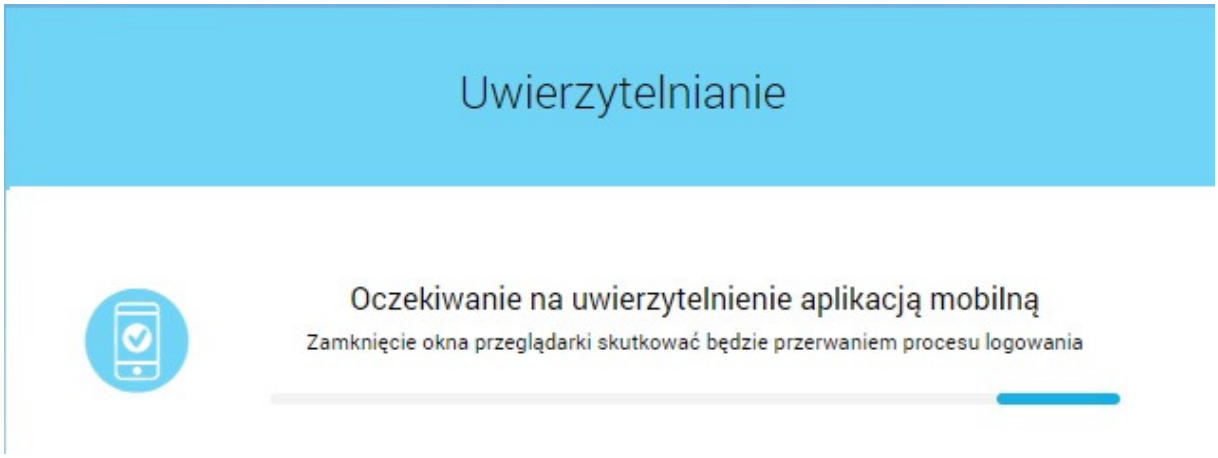


Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator użytkownika i użyć przycisku [DALEJ].

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).

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.



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”.

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.

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”.


asseco
Wyloguj
AUTORYZACJA OPERACJI
Realizacja przelewu
11.00 PLN
adrian zwykly
08 1010 1010 0088 2014 9640 0000
31 1020 0003 3862 2573 0105 5179
zwykly test przelewu
zwykły
27.08.2019
ODRZUĆ
AKCEPTUJ
274
Autoryzacje
Powiadomienia
Ustawienia


asseco
Wyloguj
AUTORYZACJA OPERACJI
Podaj PIN
Wprowadź PIN
1
2
3
4
5
6
7
8
9
0
ZATWIERDŹ
274
Autoryzacje
Powiadomienia
Ustawienia