

Rozdział 5. Logowanie do systemu

Po uruchomieniu systemu def3000/CBP wyświetlane jest okno autoryzacji:

LOGOWANIE PL

Numer Identyfikacyjny

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 DigjCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

W zależności od rodzaju wydanych użytkownikowi środków dostępu logowanie może przebiegać w następujący sposób z wykorzystaniem:

1. identyfikatora alfanumerycznego i hasła stałego,
2. identyfikatora alfanumerycznego i hasła maskowanego,
3. identyfikatora alfanumerycznego oraz hasła do tokena RSA/VASCO i aktualnego wskazania tokena,
4. identyfikatora alfanumerycznego, hasła maskowanego i aplikacji Asseco MAA
5. identyfikatora alfanumerycznego, hasła maskowanego i kodu SMS

W przypadku, gdy użytkownik posiada aktywną sesję bankowości internetowej, a następnie będzie próbował powielić ją w innej zakładce zostanie zaprezentowany komunikat informujący o nieprawidłowości takiego działania. Próba równoległej pracy w dwóch oknach skutkuje wylogowaniem użytkownika z systemu def3000/CBP.

Zdublowana zakładka

**Platforma bankowości otwarta w innym oknie**

Jesteś zalogowany do bankowości na innej zakładce przeglądarki.
Platforma bankowości może być jednocześnie otwarta tylko w jednym oknie.

Zamknij to okno i powróć do pracy w pierwotnej zakładce lub wyloguj się z bankowości (wylogowanie nastąpi na wszystkich zakładkach).

OPUŚĆ STRONĘ

WYLOGUJ Z BANKOWOŚCI

5.1. Logowanie do systemu def3000/CBP za pomocą hasła stałego, maskowanego lub tokena RSA i VASCO

W przypadku logowania za pomocą hasła stałego, hasła maskowanego, tokena RSA lub VASCO logowanie odbywa się w trybie dwukrokovym. W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny, następnie w drugim kroku dane uwierzytelniające.

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

Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

LOGOWANIE

PL

Numer Identyfikacyjny

Wpisz numer

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

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia kodu dostępu. Logowanie może przebiegać z wykorzystaniem hasła stałego, hasła maskowanego, tokena RSA lub tokena VASCO (model GO3).

Jako kod uwierzytelniający mogą zatem zostać użyte odpowiednio:

- hasło:

← LOGOWANIE

Kod dostępu

ZALOGUJ

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
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

- wybrane znaki z hasła (hasło maskowane) - w polu **Kod dostępu** należy wprowadzić losowo wybrane wymagane pozycje z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

← LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

ZALOGUJ

Pamiętaj o podstawowych zasadach bezpieczeństwa.

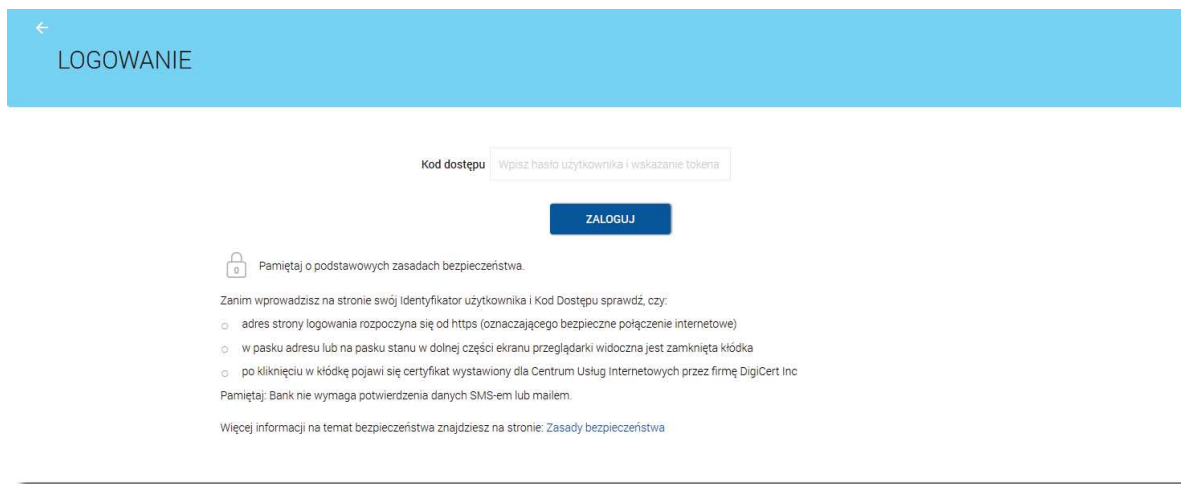
Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- 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
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc

Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

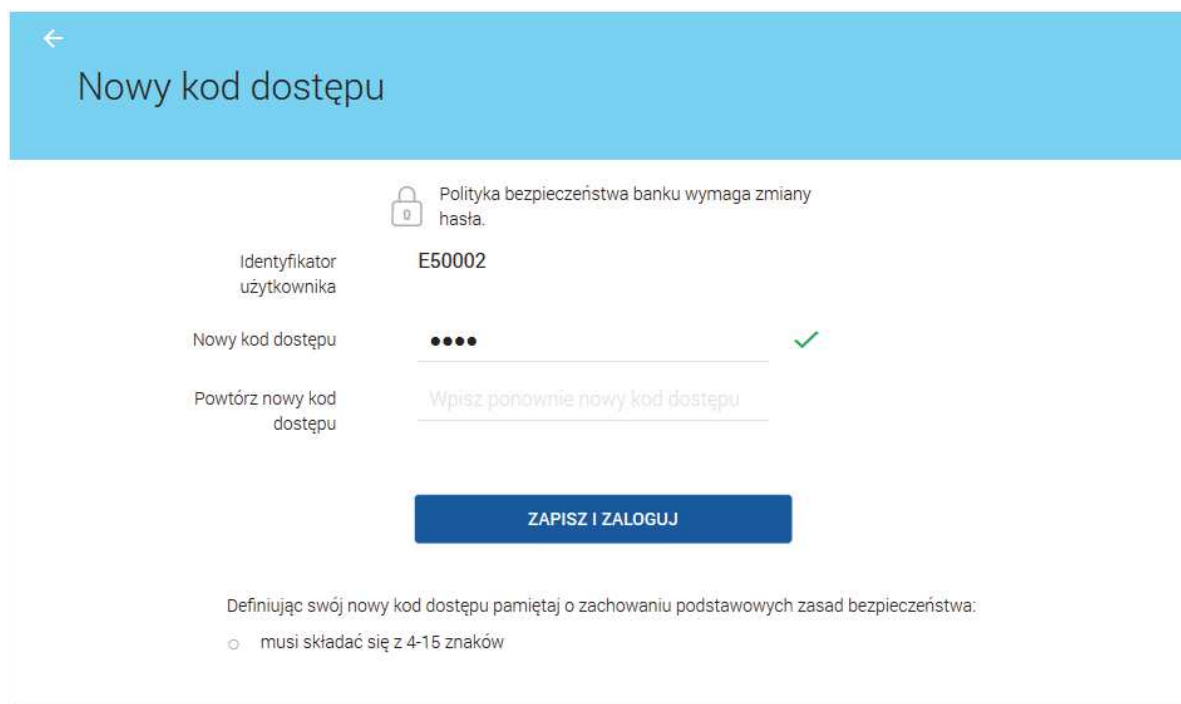
- hasło do tokena łącznie ze wskazaniem tokena RSA/VASCO (model GO3):



Za pomocą przycisku  możliwy jest powrót do poprzedniej strony logowania.

Po wprowadzeniu (w polu **Kod dostępu**) poprawnego kodu uwierzytelniającego należy użyć przycisku [ZALOGUJ]. System weryfikuje wprowadzone dane i jeżeli stwierdzi ich poprawność użytkownik zostanie zalogowany.

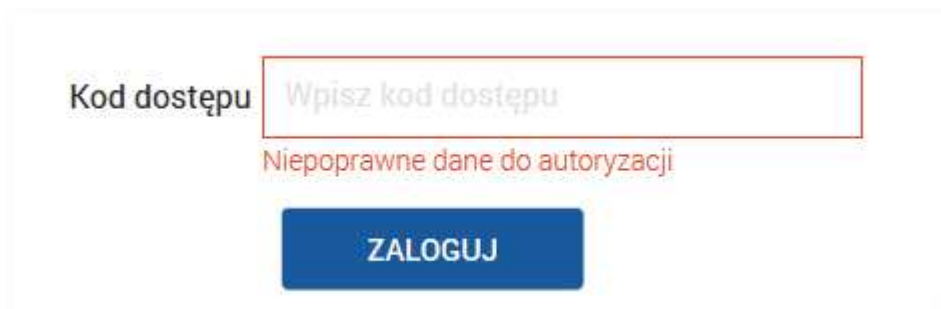
Jeżeli klient loguje się pierwszy raz, po wprowadzeniu identyfikatora a następnie hasła oraz wyborze przycisku [ZALOGUJ] zostanie zaprezentowana formatka *Nowy kod dostępu* wymuszająca zmianę hasła do logowania. Należy wpisać dwukrotnie nowe hasło oraz nacisnąć przycisk [ZAPISZ I ZALOGUJ].



W przypadku, gdy usługa **sms.zalogowanie.uzytkownika.cbp** ustawiona jest na wartość *true* oraz w aplikacji BankAdmin użytkownikowi udostępniona została opcja *Informacja o zalogowaniu (SMS)* wówczas do użytkownika zostanie wysłany SMS informujący o pozytywnym zalogowaniu do aplikacji def3000/CBP.

W przypadku błędnie wprowadzonych danych autoryzacyjnych system wyświetla komunikat: *"Niepoprawne*

dane do autoryzacji" i nie pozwala zalogować się do systemu.



The screenshot shows a login interface with the following elements:

- A label "Kod dostępu" (Access code) on the left.
- A text input field containing the placeholder text "Wpisz kod dostępu" (Enter access code).
- A red error message below the input field: "Niepoprawne dane do autoryzacji" (Incorrect authorization data).
- A blue button labeled "ZALOGUJ" (Log in) below the error message.

5.2. Logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA

Niniejszy rozdział opisuje możliwość logowania do systemu def3000/CBP za pomocą aplikacji Asseco MAA. Użytkownik podczas logowania może dysponować aktywnym sparowanym urządzeniem lub może podczas logowania do systemu def3000/CBP dopiero parować urządzenie. Rozdział przedstawia opis obu wariantów z uszczegółowieniem poszczególnych przypadków.

W pierwszej części rozdziału umieszczono opis logowania za pomocą **aktywnego sparowanego urządzenia** uwzględniający trzy przypadki:

- Logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie z logowania hasłem maskowanym na logowanie mobilne
- Pierwsze logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie z logowania hasłem stałym, tokenem RSA lub VASCO na logowanie mobilne
- Kolejne logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA

W drugiej części rozdziału znajduje się opis **procesu parowania urządzenia podczas logowania do systemu def3000/CBP** uwzględniającego przypadki :

- Logowanie do systemu def3000/CBP, gdy użytkownik nie posiada sparowanego aktywnego urządzenia mobilnego.
- Użytkownik loguje się po raz pierwszy do systemu def3000/CBP i nie posiada sparowanego urządzenia lub loguje się za pomocą hasła zresetowanego (tymczasowego) i nie posiada sparowanego urządzenia mobilnego.

5.2.1. Logowanie do systemu def3000/CBP za pomocą aktywnego i sparowanego urządzenia mobilnego

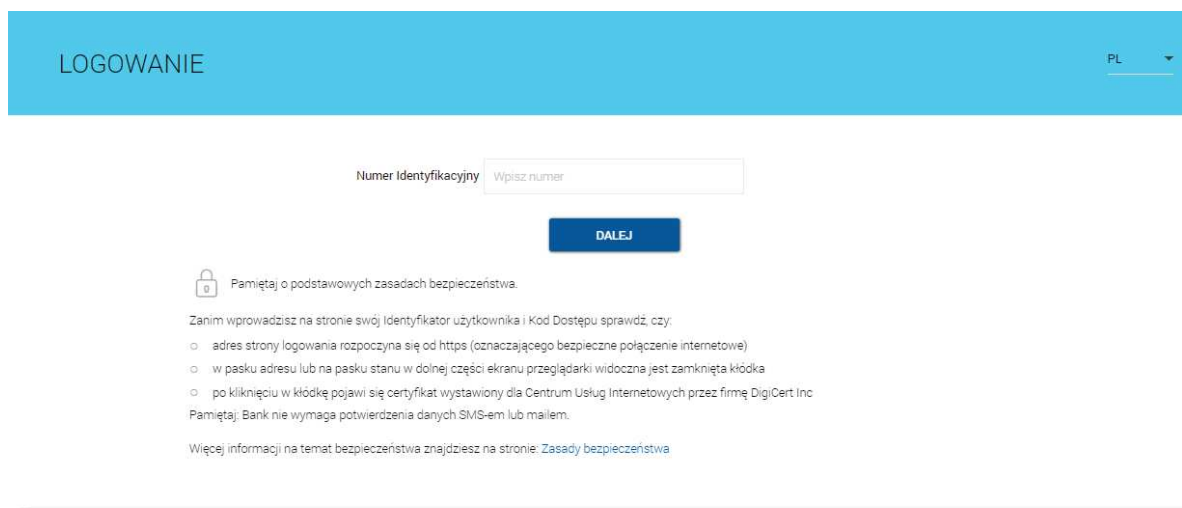
5.2.1.1. Logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie z logowania hasłem maskowanym na logowanie mobilne



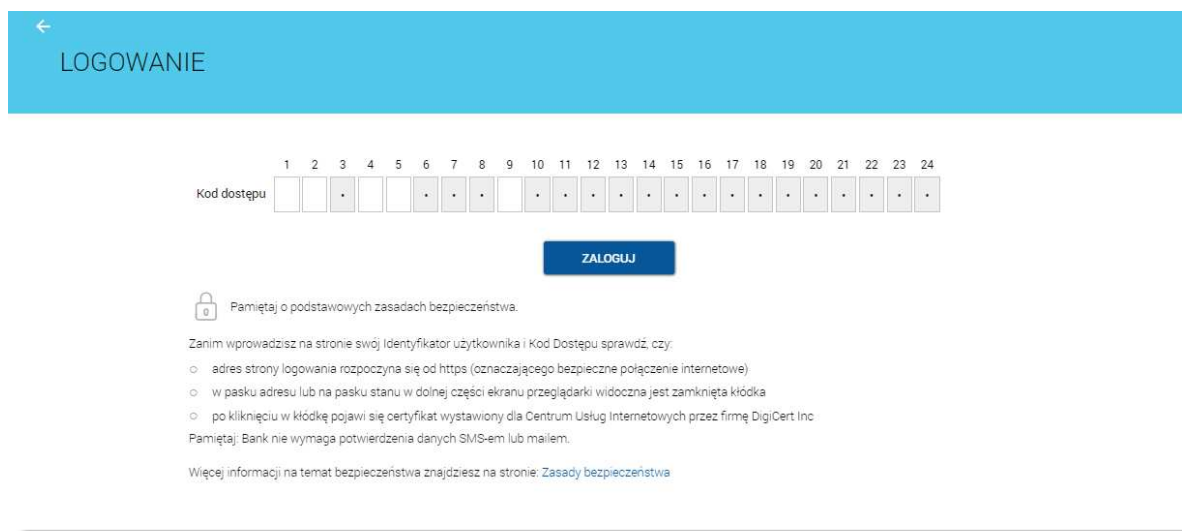
Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **hasła maskowanego**, wówczas dotychczasowe hasło służy do logowania za pomocą aplikacji Asseco MAA.

Niniejszy rozdział opisuje logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie sposobu logowania z logowania hasłem maskowanym na logowanie mobilne przy założeniu, że Klient posiada aktywne sparowane urządzenie.

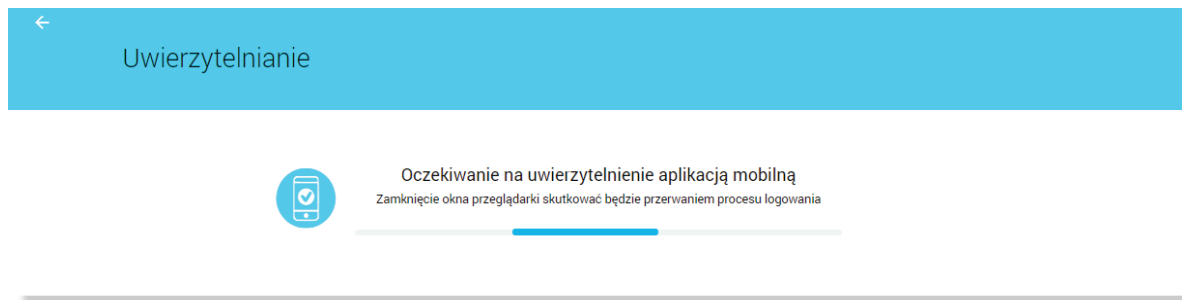
W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:



Po wyborze przycisku [ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu.



Na sparowane urządzenie zostaje wysłane powiadomienie z informacją o autoryzacji logowania do systemu.



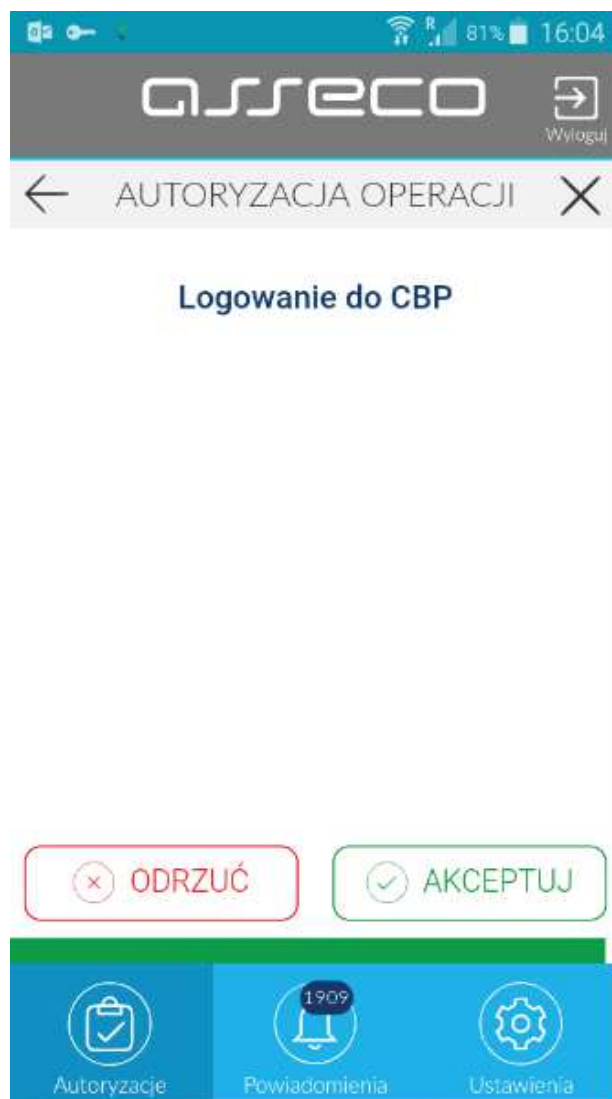
Stuknięcie w powiadomienie przenosi do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA PINem ustawionym podczas rejestracji urządzenia.



Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



Po wyborze autoryzacji zostają wyświetlone jej szczegóły:



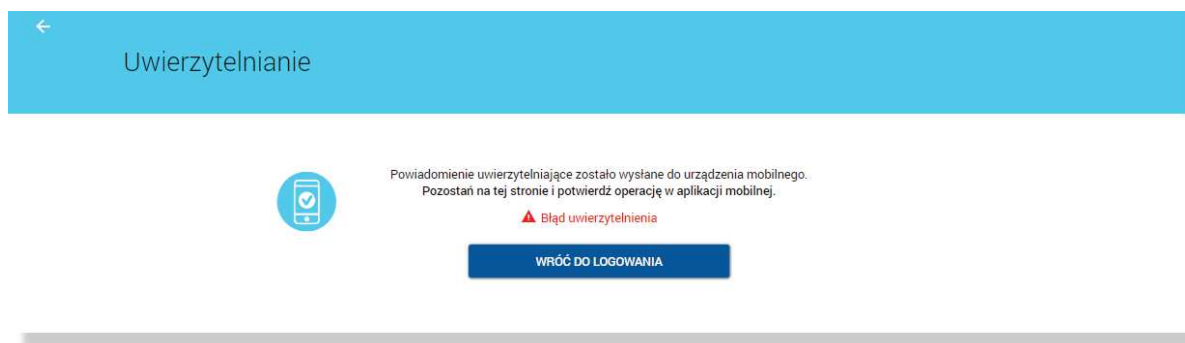
Po akceptacji autoryzacji zostaje wyświetlone potwierdzenie i następuje zalogowanie Klienta do systemu def3000/CBP.



W przypadku:

- odrzucenia autoryzacji w aplikacji Asseco MAA przez Klienta lub
- upłynięcia czasu na autoryzację

prezentowany jest komunikat:



5.2.1.2. Pierwsze logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie z logowania hasłem stałym, tokenem RSA lub VASCO na logowanie mobilne

Niniejszy rozdział opisuje logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA po zmianie sposobu logowania z logowania hasłem stałym, tokenem RSA lub VASCO na logowanie mobilne przy założeniu, że Klient posiada aktywne sparowane urządzenie.



Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **hasła stałego, tokena RSA lub VASCO**, wówczas Pracownik banku generuje **tymczasowe hasło mobilne**, które zostaje wysłane do Klienta za pomocą wiadomości SMS.

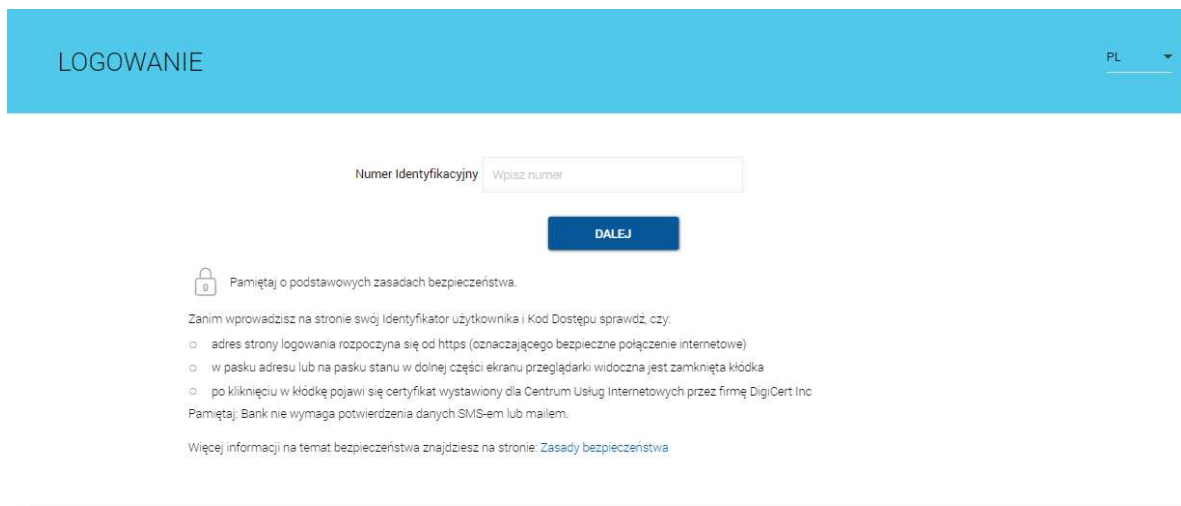
Hasło tymczasowe mobilne wymaga zmiany podczas pierwszego logowania przy pomocy aplikacji Asseco MAA.



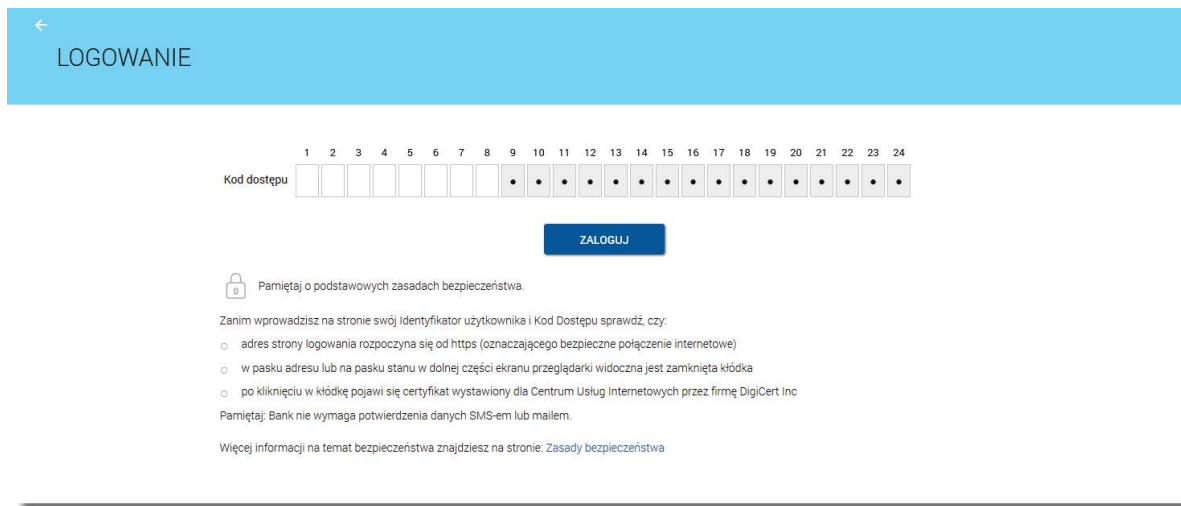
Jeżeli hasło mobilne użytkownika jest **zablokowane lub nieaktywne** (minął czas ważności hasła) - hasło mobilne użytkownika może zostać zresetowane

Nowe hasło tymczasowe mobilne zostaje wysłane na numer SMS Klienta. Podczas pierwszego logowania aplikacją mobilną po podaniu hasła tymczasowego mobilnego wymagane jest podanie nowego hasła mobilnego.

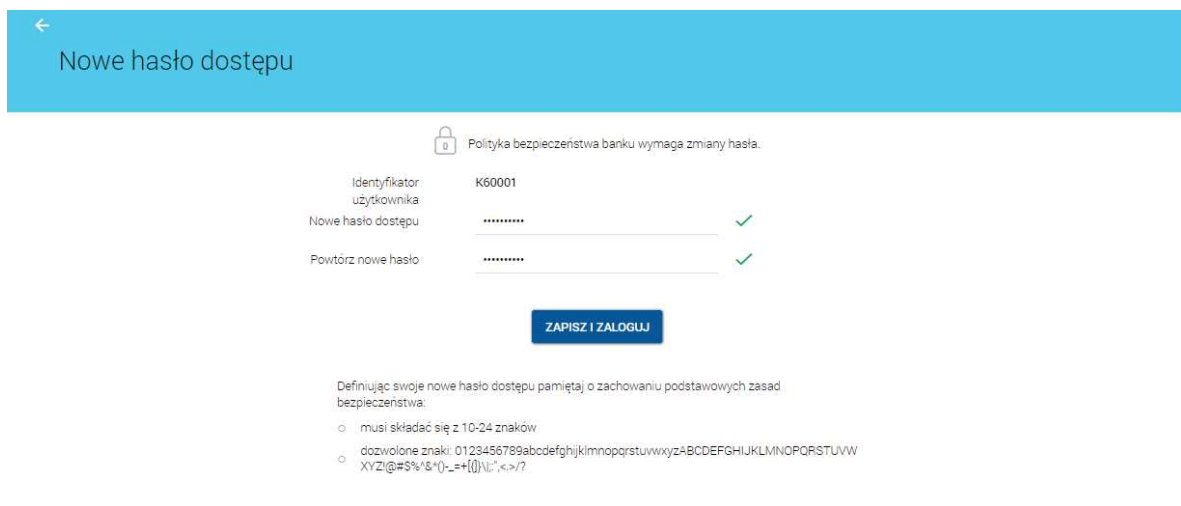
W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



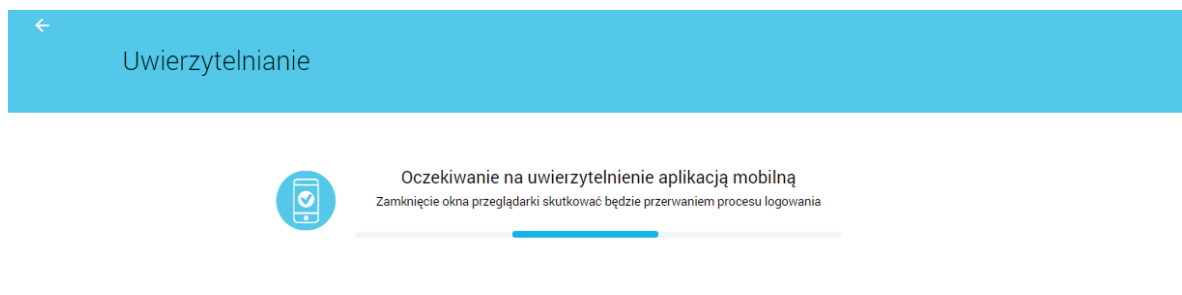
Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia **tymczasowego hasła mobilnego**. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:



Po wyborze przycisku [ZALOGUJ] zostaje wyświetlona formatka zmiany hasła:



W oknie należy wprowadzić nowe hasło spełniające wymogi polityki bezpieczeństwa znajdujące się w dolnej części formatki. Po powtórzeniu hasła i wyborze przycisku [ZAPISZ I ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu:



Na sparowane urządzenie zostaje wysłany push z informacją o autoryzacji logowania do systemu.



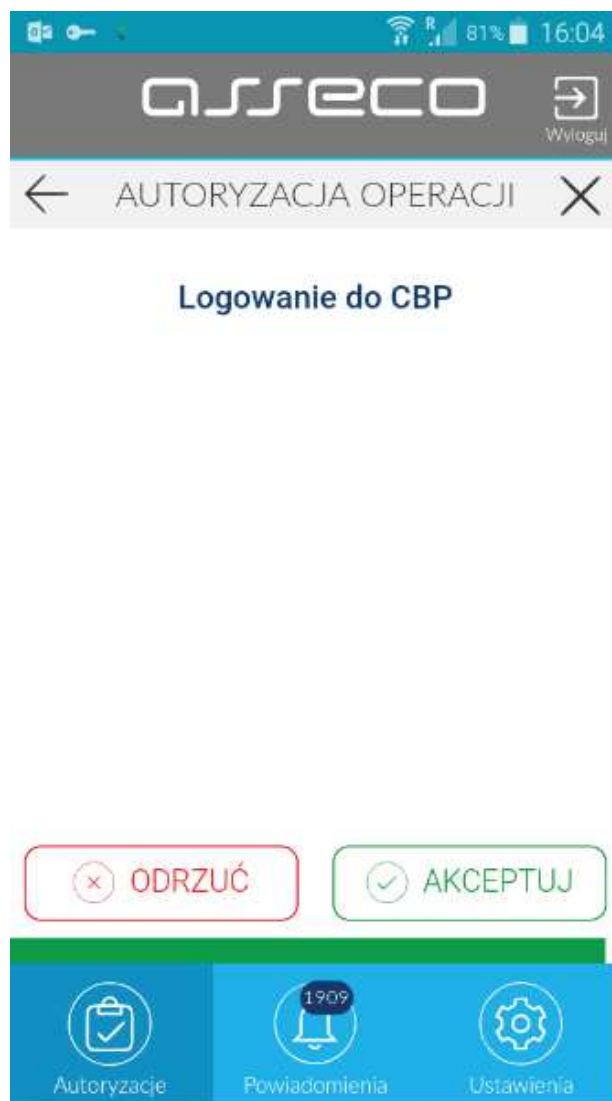
Stuknięcie w push przenosi do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA PINem ustawionym podczas rejestracji urządzenia.



Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



Po wyborze autoryzacji zostają wyświetlone jej szczegóły:



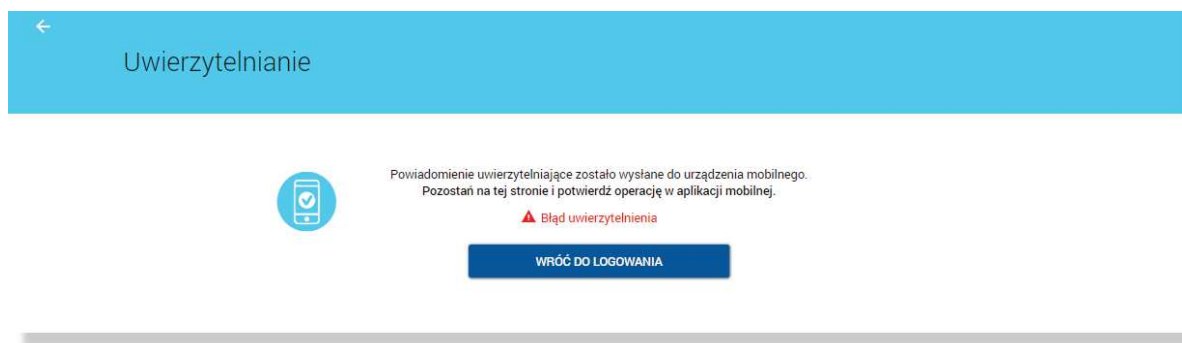
Po akceptacji autoryzacji zostaje wyświetlone potwierdzenie i następuje zalogowanie Klienta do systemu def3000/CBP.



W przypadku:

- odrzucenia autoryzacji w aplikacji Asseco MAA przez Klienta lub
- upłynięcia czasu na autoryzację

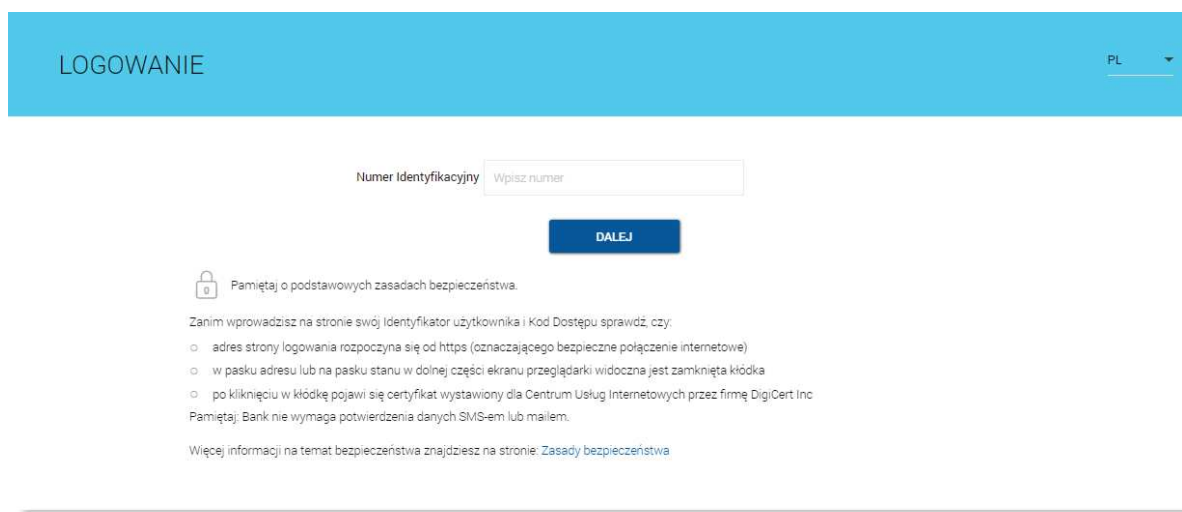
prezentowany jest komunikat:



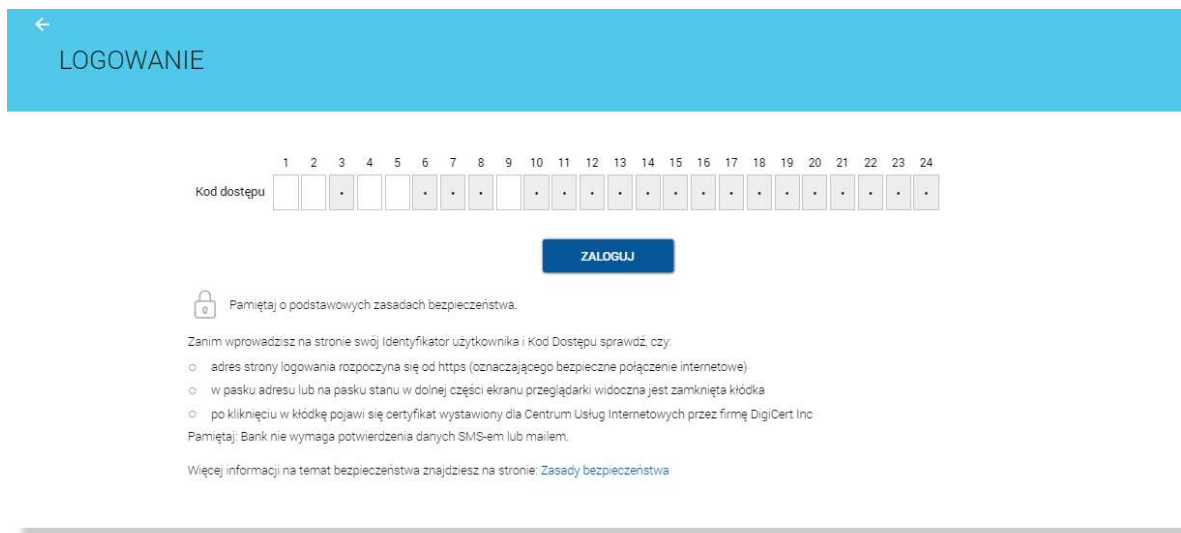
5.2.1.3. Kolejne logowanie do systemu def3000/CBP za pomocą aplikacji Asseco MAA

Klient może logować się do systemu def3000/CBP za pomocą aplikacji mobilnej Asseco MAA, jeżeli posiada sparowane aktywne urządzenie oraz hasło mobilne.

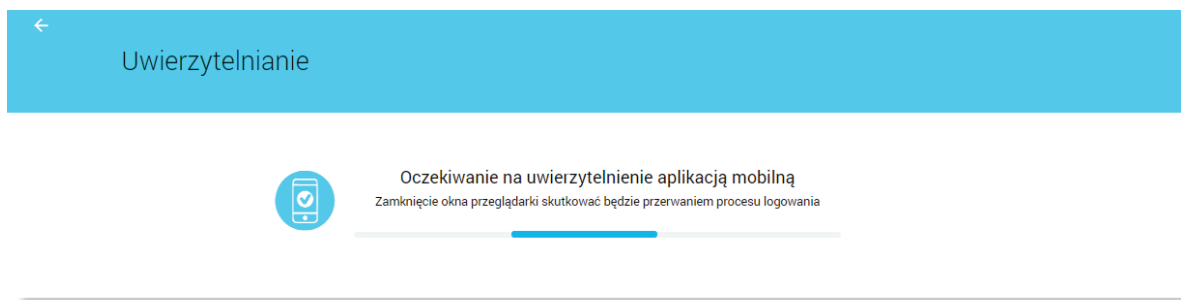
W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



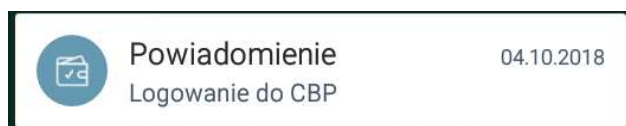
Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte i zastąpione znakiem •. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:



Po wyborze przycisku [ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu.



Na sparowane urządzenie zostaje wysłany push z informacją o autoryzacji logowania do systemu.



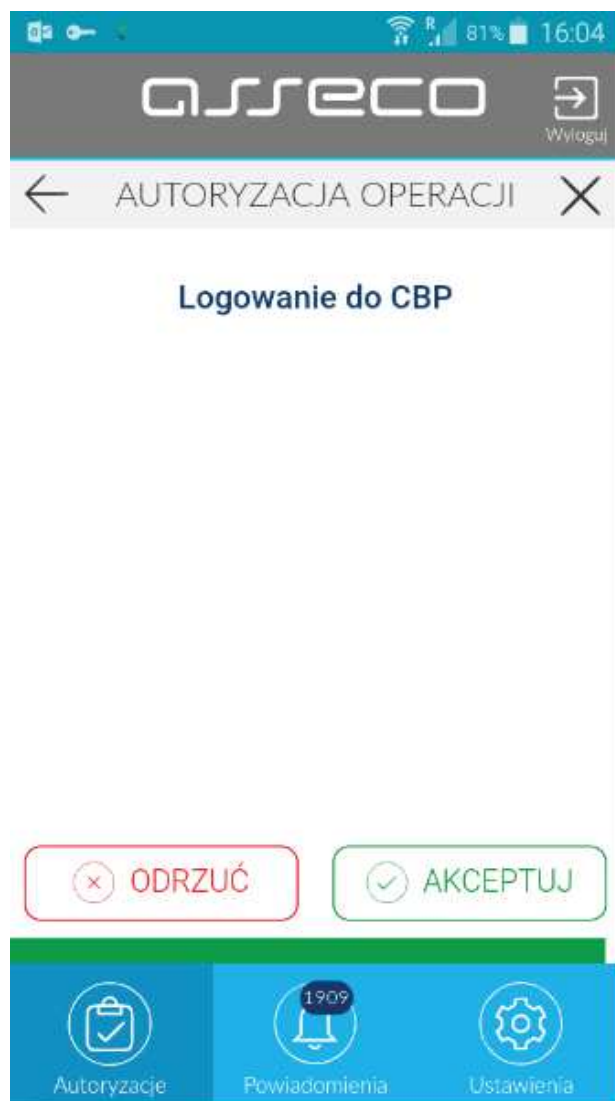
Stuknięcie w push przenosi do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA PINem ustawionym podczas rejestracji urządzenia.



Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja.



Po wyborze autoryzacji zostają wyświetlone jej szczegóły:



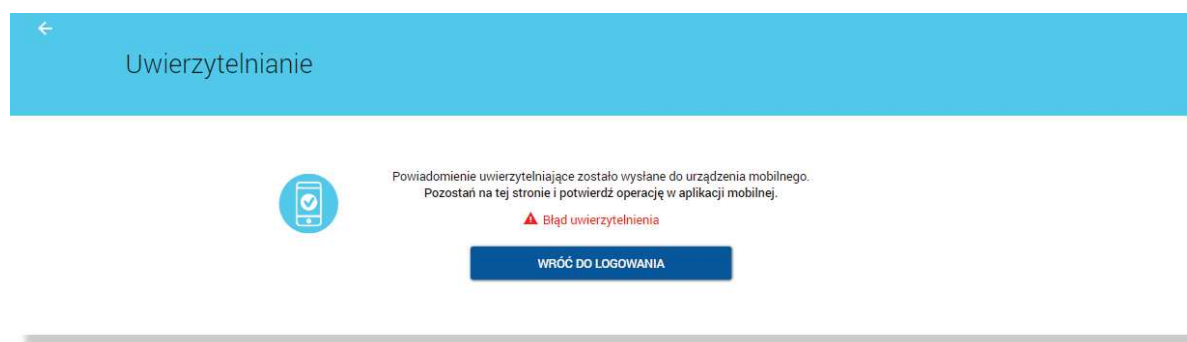
Po akceptacji autoryzacji zostaje wyświetlone potwierdzenie i następuje zalogowanie Klienta do systemu def3000/CBP.



W przypadku:

- odrzucenia autoryzacji w aplikacji Asseco MAA przez Klienta lub
- upływu czasu na autoryzację

prezentowany jest komunikat:



5.2.2. Aktywacja urządzenia mobilnego w procesie logowania do systemu def3000/CBP

W niniejszym rozdziale przedstawiono opis procesu parowania urządzenia za pomocą aplikacji mobilnej Asseco MAA podczas logowania do systemu def3000/CBP w przypadku, gdy użytkownik nie posiada aktywnego urządzenia mobilnego.




Możliwość parowania urządzenia w procesie logowania wymaga włączenia usługi ASSIGN_DEVICE_WHEN_AUTHORIZE na bazie Guardiania

- Logowanie do systemu def3000/CBP, gdy Klient nie posiada sparowanego aktywnego urządzenia mobilnego.
- Klient loguje się po raz pierwszy do systemu def3000/CBP i nie posiada sparowanego urządzenia lub loguje się za pomocą hasła zresetowanego (tymczasowego) i nie posiada sparowanego urządzenia mobilnego.
- Przypadek, gdy w systemie wyłączono możliwość parowania urządzenia w procesie logowania i użytkownik nie posiada sparowanego urządzenia oraz jest nowym użytkownikiem.
- Przypadek, gdy w systemie wyłączono możliwość parowania urządzenia podczas logowania i użytkownik nie posiada sparowanego urządzenia mobilnego.

5.2.2.1. Parowanie urządzenia podczas logowania do systemu def3000/CBP

W przypadku, gdy Klient nie posiada sparowanego urządzenia po podaniu loginu i hasła Asseso MAA maskowanego prezentowany jest pierwszy krok parowania urządzenia.


←
Urządzenie autoryzujące



Do autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAA

Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store

POSIADAM APLIKACJĘ

 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.

Pamiętaj, Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

Po wyborze przycisku [POSIADAM APLIKACJĘ] zostanie wyświetlona formatka z drugim krokiem procesu, na której prezentowany jest kod aktywacyjny, który należy wprowadzić w aplikacji mobilnej Asseco MAA podczas rejestracji urządzenia. Pasek postępu odlicza czas pozostały na parowanie.

←
Uwierzytelnianie

417 985

Kod aktywacyjny

Wprowadź powyżej wygenerowany kod w aplikacji mToken Asseco MAA

Kod jest ważny przez 5 minut

←
Uwierzytelnianie

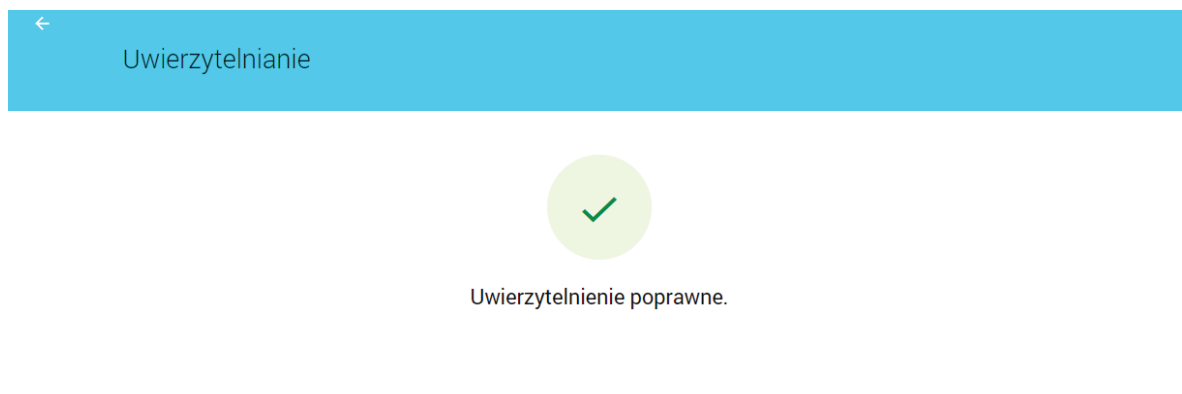
417 985

Kod aktywacyjny

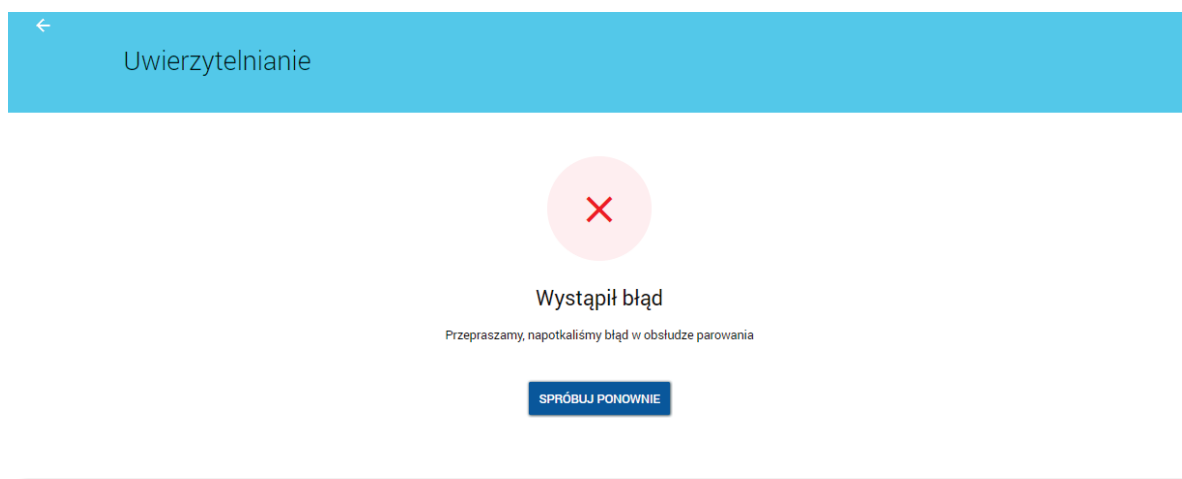
Wprowadź powyżej wygenerowany kod w aplikacji mToken Asseco MAA

Kod jest ważny przez 5 minut

Po aktywacji urządzenia mobilnego w aplikacji def3000/CBP prezentowane jest potwierdzenie poprawnego sparowania urządzenia. Następuje zalogowanie do systemu def3000/CBP.



W przypadku, gdy urządzenie nie zostało sparowane - przykładowo upłynął czas na parowanie w systemie def3000/CBP prezentowany jest komunikat jak na poniższym ekranie.



5.2.2.2. Parowanie urządzenia podczas pierwszego logowanie do systemu def3000/CBP lub po resecie hasła (za pomocą hasła tymczasowego).

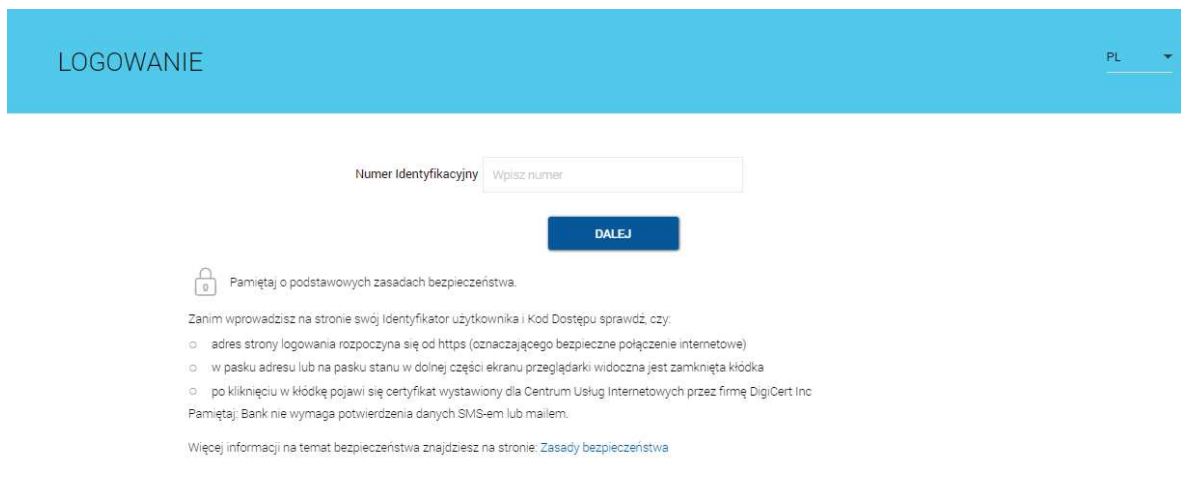


Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **hasła stałego, tokena RSA lub VASCO**, wówczas Pracownik banku generuje **tymczasowe hasło mobilne**, które zostaje wysłane do Klienta za pomocą wiadomości SMS.

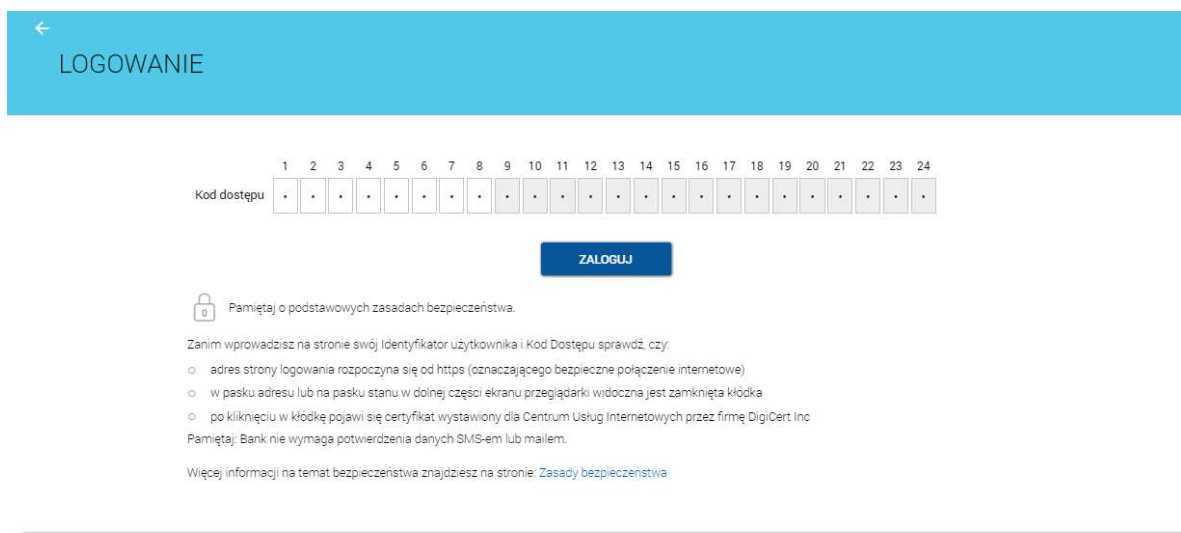


Jeżeli hasło mobilne użytkownika jest **zablokowane lub nieaktywne** (minął czas ważności hasła) - hasło mobilne użytkownika może zostać zresetowane

W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



Logowanie do systemu def3000/CBP odbywa się za pomocą hasła tymczasowego, które użytkownik otrzymał za pomocą wiadomości SMS.



Hasło tymczasowe mobilne wymaga zmiany podczas pierwszego logowania przy pomocy aplikacji Asseco MAA. Po wyborze przycisku [ZALOGUJ] zostaje wyświetlona formatka zmiany hasła:

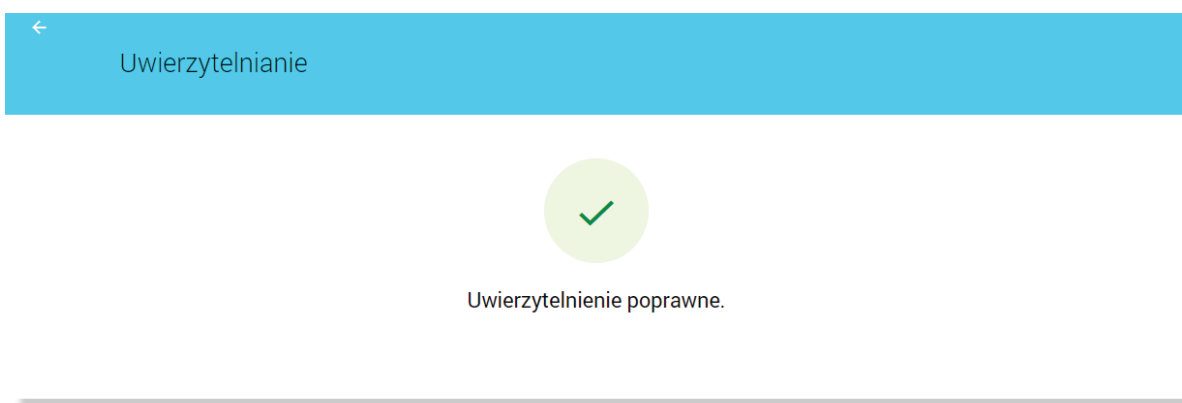
Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia **tymczasowego hasła mobilnego**. Przy wpisywaniu hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

W oknie należy wprowadzić nowe hasło spełniające wymogi polityki bezpieczeństwa znajdujące się w dolnej części formatki. Po powtórzeniu hasła i wyborze przycisku [ZAPISZ I ZALOGUJ] następuje przejście do okna umożliwiającego sparowanie urządzenia mobilnego za pomocą aplikacji Asseco MAA.

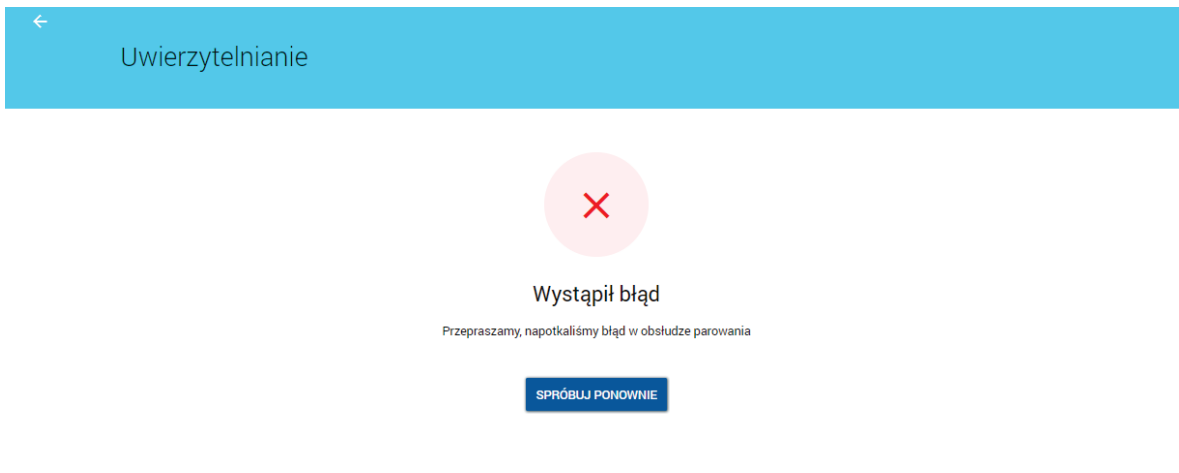
Po wyborze przycisku [POSIADAM APLIKACJĘ] zostanie wyświetlona formatka z drugim krokiem procesu, na której prezentowany jest kod aktywacyjny, który należy wprowadzić w aplikacji mobilnej Asseco MAA podczas rejestracji urządzenia. Pasek postępu odlicza czas pozostały na parowanie.



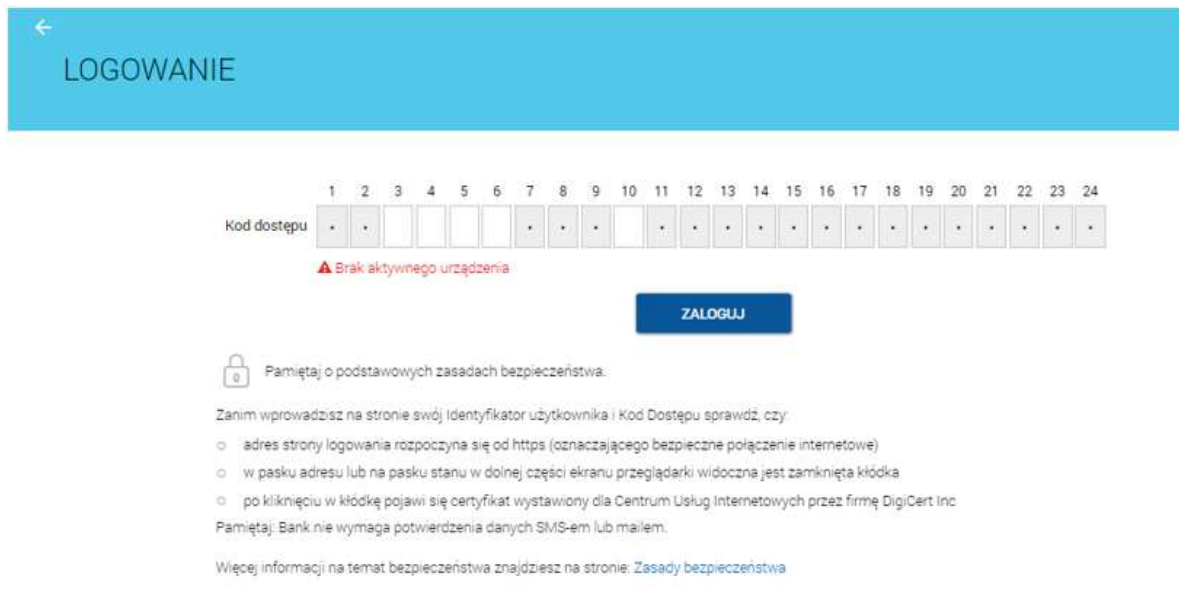
Po aktywacji urządzenia mobilnego w aplikacji def3000/CBP prezentowane jest potwierdzenie poprawnego sparowania urządzenia. Następuje zalogowanie do systemu def3000/CBP.



W przypadku, gdy urządzenie nie zostało sparowane - przykładowo upłynął czas na parowanie w systemie def3000/CBP prezentowany jest komunikat jak na poniższym ekranie.



W przypadku, gdy wyłączono możliwość parowania urządzenia w procesie logowania i użytkownik nie posiada sparowanego urządzenia po podaniu loginu i hasła prezentowany jest komunikat "Brak aktywnego urządzenia".



5.3. Logowanie za pomocą hasła maskowanego i kodu SMS

Niniejszy rozdział przedstawia proces logowania do systemu def3000/CBP za pomocą metody "hasło maskowane i kod SMS". Opis przedstawia:

- pierwsze logowanie do systemu def3000/CBP za pomocą tymczasowego hasła maskowanego i kodu SMS
- kolejne logowanie do systemu def3000/CBP za pomocą nowego hasła maskowanego i kodu SMS



Jeżeli użytkownik dotychczas logował się do def3000/CBP za pomocą **hasła stałego, tokena RSA lub VASCO**, wówczas Pracownik banku generuje **tymczasowe hasło maskowane**, które zostaje wysłane do Klienta za pomocą wiadomości SMS. Hasło tymczasowe maskowane wymaga zmiany podczas pierwszego logowania.



Jeżeli Klient dotychczas logował się hasłem maskowanym i **hasło maskowane Klienta zostało zmigrowane** proces pierwszego logowania metodą "hasło maskowane i kod SMS" nie wymaga zmiany hasła maskowanego.



Jeżeli Klient dotychczas logował się hasłem maskowanym i hasło maskowane Klienta **nie zostało zmigrowane** proces pierwszego logowania metodą "hasło maskowane i kod SMS" wymaga zmiany hasła maskowanego.



Jeżeli hasło maskowane użytkownika jest **zablokowane lub nieaktywne** (minął czas ważności hasła) - hasło maskowane użytkownika może zostać zresetowane

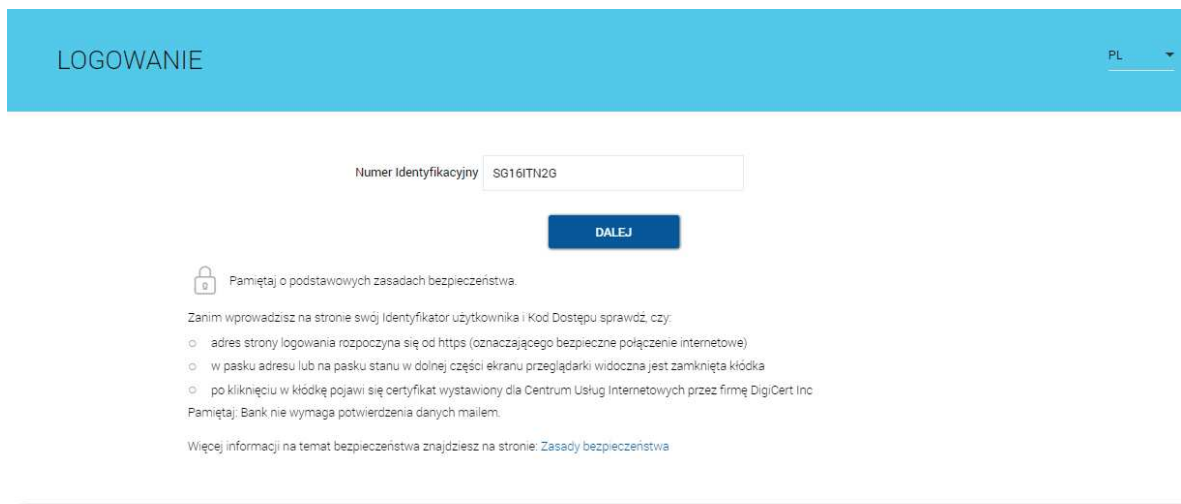
5.3.1. Pierwsze logowanie do systemu def3000/CBP za pomocą tymczasowego hasła maskowanego i kodu SMS

Niniejszy rozdział opisuje pierwsze logowanie do systemu def3000/CBP za pomocą metody "hasło maskowane i kod SMS" po zmianie sposobu logowania z logowania:

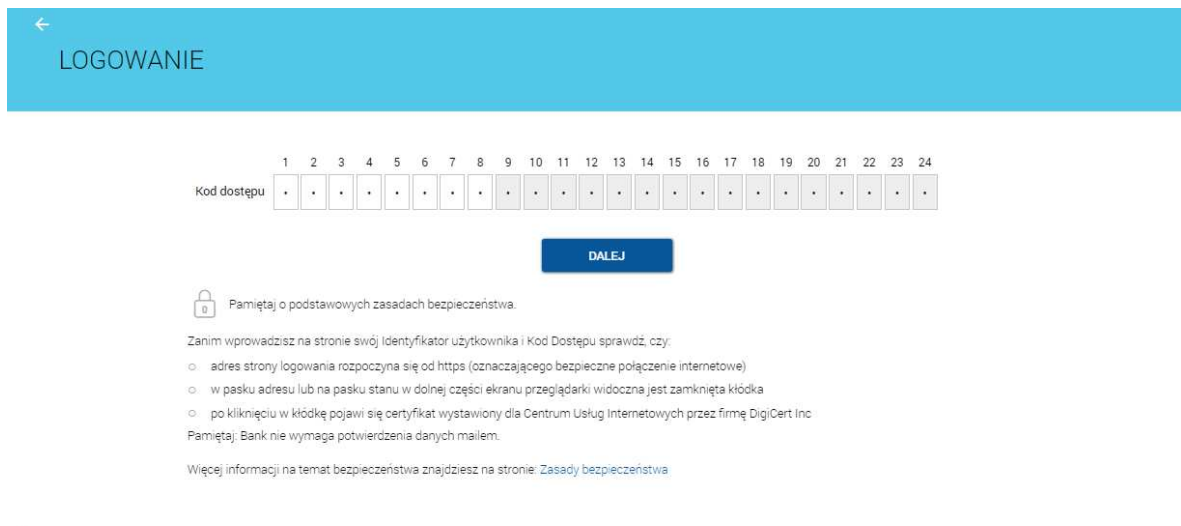
- hasłem stałym, tokenem RSA lub VASCO,
- hasłem maskowanym, jeżeli hasło maskowane Klienta **nie zostało zmigrowane**

Podczas pierwszego logowania metodą "hasło maskowane i kod SMS" wymagana jest zmiana tymczasowego hasła maskowanego. Hasło tymczasowe maskowane zostaje wysłane na numer telefonu podany w danych Klienta.

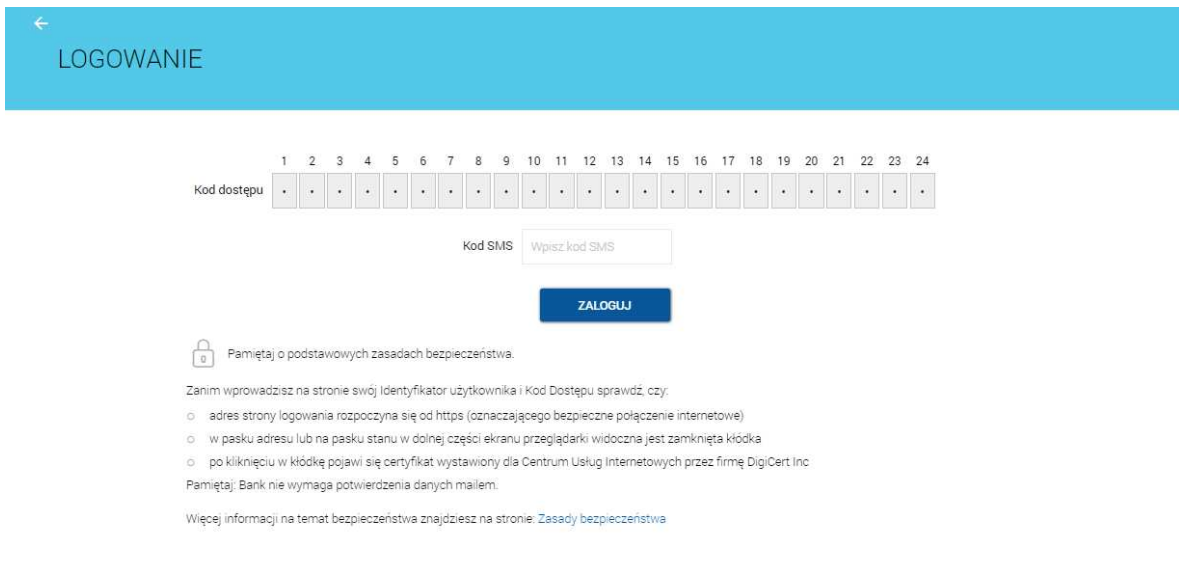
Klient, który pierwszy raz loguje się do systemu def3000/CBP za pomocą metody "hasło maskowane i kod SMS" w pierwszym kroku w polu Numer Identyfikacyjny wprowadza identyfikator alfanumeryczny. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia tymczasowego hasła maskowanego. Przy wprowadzaniu tymczasowego hasła maskowanego, po wpisaniu znaku następuje automatyczne przeskoczenie do kolejnego pola:

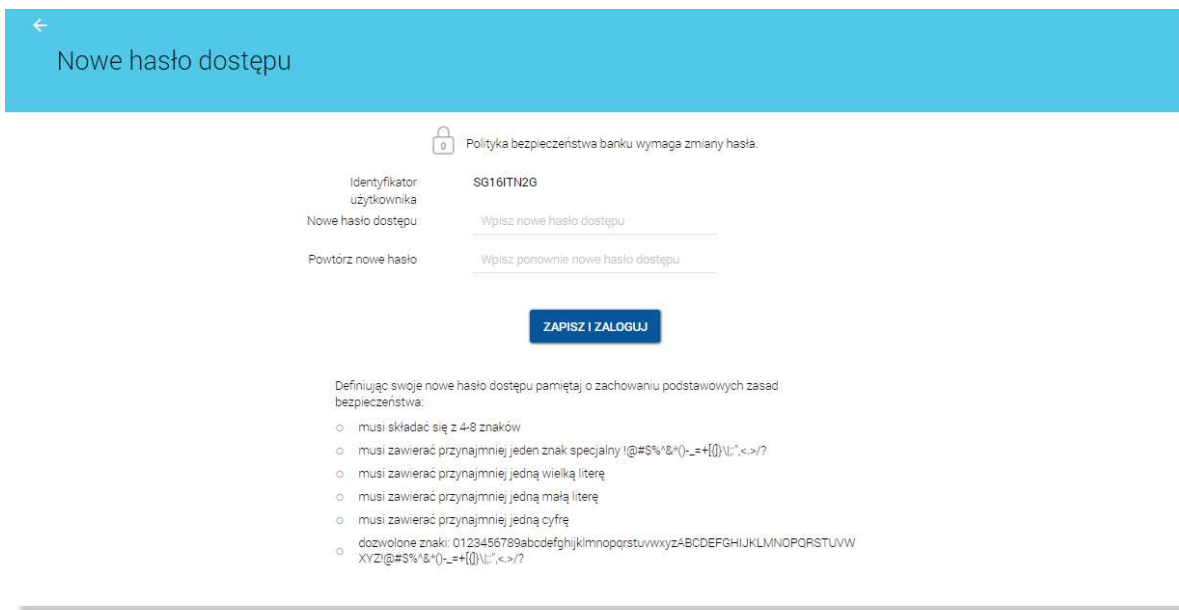


Po wprowadzeniu tymczasowego hasła maskowanego i wybraniu [DALEJ] podane dane są weryfikowane. Jeżeli tymczasowe hasło maskowane jest poprawne na formacie zaprezentowane zostaje pole do wpisania kodu SMS. W polu Kod SMS należy wprowadzić otrzymany kod na podany w danych Klienta numer telefonu.

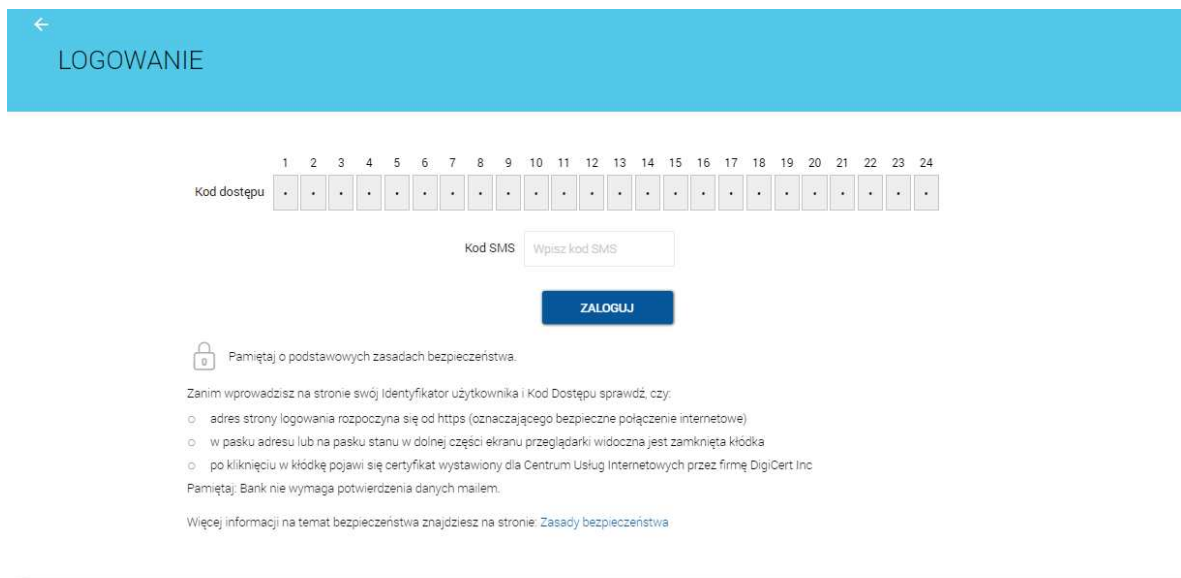


Hasło tymczasowe maskowane wymaga zmiany podczas pierwszego logowania. Jeżeli minął czas ważności hasła tymczasowego maskowane - hasło maskowane Klienta może zostać zresetowane i przesłane na podany w danych Klienta numer telefonu.

Po wyborze przycisku [ZALOGUJ] zostaje wyświetlona formatka zmiany hasła:



W oknie należy wprowadzić nowe hasło spełniające wymogi polityki bezpieczeństwa znajdujące się w dolnej części formatki. Po powtórzeniu hasła i wybraniu [ZAPISZ I ZALOGUJ] należy wprowadzić nowy kod SMS wysłany na numer telefonu podany w danych Klienta.

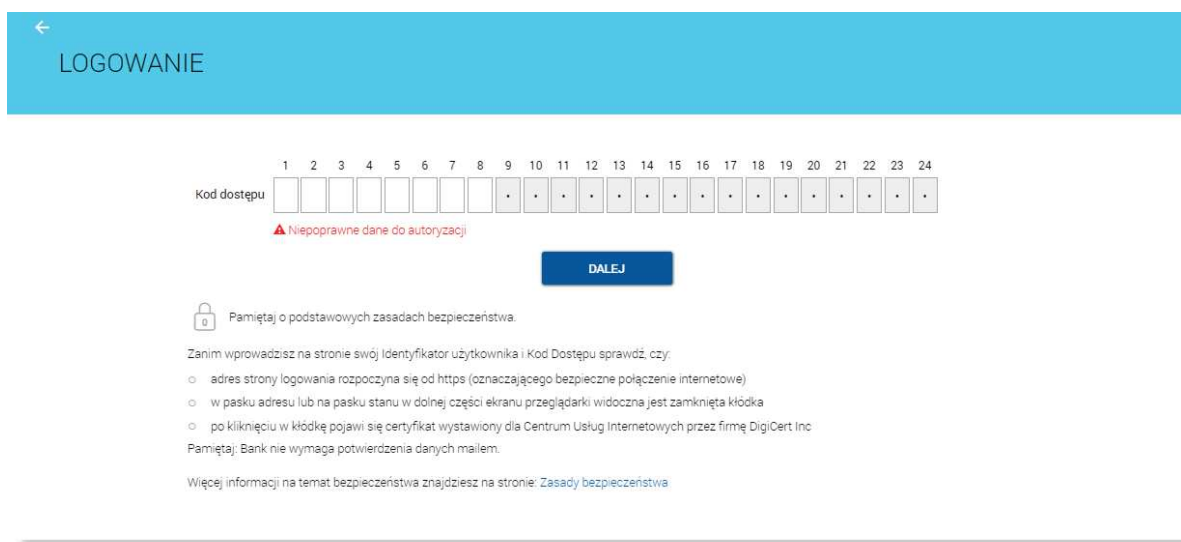


Po wybraniu [ZALOGUJ] i poprawnej weryfikacji następuje zalogowanie do systemu.

W przypadku:

- podania niepoprawnego tymczasowego hasła maskowanego,
- podania niepoprawnego kodu SMS przed zmianą tymczasowego hasła maskowanego,
- gdy tymczasowe hasło maskowane zostało zablokowane,
- gdy ważność tymczasowego hasła maskowanego wygasła

zostaje wyświetlony komunikat "Niepoprawne dane do autoryzacji":



W przypadku podania niepoprawnego kodu SMS, po zmianie hasła tymczasowego maskowanego na nowe hasło maskowane, zostaje wyświetlony komunikat "Niepoprawne dane do autoryzacji":

← LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
.

▲ Niepoprawne dane do autoryzacji

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

Pamiętaj! Bank nie wymaga potwierdzenia danych mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#)

5.3.2. Kolejne logowanie do systemu def3000/CBP za pomocą hasła maskowanego i kodu SMS

Niniejszy rozdział przedstawia proces logowania metodą "hasło maskowane i kod SMS" po pierwszym logowaniu do systemu def3000/CBP podczas którego Klient ustawił nowe hasło maskowane.



Jeżeli Klient dotychczas logował się hasłem maskowanym i **hasło maskowane Klienta zostało zmigrowane** proces pierwszego logowania metodą "hasło maskowane i kod SMS" nie wymaga zmiany hasła maskowanego i przebiega zgodnie z poniższym opisem.

Logowanie metodą "hasło maskowane i kod SMS" odbywa się w trybie trzykrokowym. W pierwszym kroku użytkownik wprowadza swój identyfikator alfanumeryczny, następnie podaje hasło maskowane i zatwierdza proces logowania kodem SMS.

Aby zalogować się do systemu należy w polu Numer Identyfikacyjny wprowadzić identyfikator alfanumeryczny użytkownika i użyć przycisku [DALEJ]. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tę wartość jako jednakową. Wpisany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.