Rozdział 5. Logowanie do systemu

areco

Po uruchomieniu systemu def3000/CBP wyświetlane jest okno autoryzacji:

LOGOWANIE	PL 🔻
Numer Identyfikacyjny Wpisz numer 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 klódka po kliknięciu w klódkę 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 	

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 załogowany 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 dwukrokowym. W pierwszym kroku użytkownik wprowadza swój identyfikatora 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 tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

LOGOWANIE	PL 💌
Numer Identyfikacyjny Wpisz numer DALEJ	
Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na stronie śwój 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 SIMS-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 Wpisz 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:

LO	GOWANI	IE																						
	Kod dostępu	1	2 3	4	•	6 •	7	8	9	10 1	1 12	13	14 •	15	16 •	17 •	18	19 •	20	21	22	23	24 •	
	D Pamięt	aj o pod:	stawov	ych za	isadac	h bezj	piecz	eństwa	а,		ZAI	.ogu,	J											
	Zanim wprowa o adres stror o w pasku ad o po kliknięc	dzisz na ny logow dresu lut ilu w kłóc	stronie ania ro na pa: Ikę poja	swój l zpoczy sku sta awi się	dentyf rna się nu w c certyfi	ikator od ht Iolnej kat w	użytł tps (c częśc ystaw	kownił Iznacz ci ekra Viony c	ta i Ko ające nu pr. Ila Ce	od Dos ego be zegląc entrum	itępu s zpieczi arki wi Usług	prawo ne poł idoczr Interr	lź, czy ączer na jest netow	r: ile inte : zaml ych p	erneto knięta rzez f	owe) a kłóc îrmę	lka DigiC	ert In	с					
	Pamiętaj: Bank Więcej informa	nie wym Icji na ter	naga po mat be:	otwierd: zpiecze	zenia (eństwa	danyc znajc	h SM: Iziesz	S-em l : na sti	ub m ronie:	ailem. Zasao	ly bezt	piecze	ństwa	1										

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



< LOGOWANIE	
	Kod dostępu Wpisz hasło użytkownika i wakażanie tokena 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 kródka 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 maliem. Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa

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].

	 Polityka bezpieczeństwa banku wymaga z 	rmiany
	hasła.	
ldentyfikator użytkownika	E50002	
Nowy kod dostępu	••••	\checkmark
Powtórz nowy kod dostępu		
	ZAPISZ I ZALOGUJ	
Definiujac swój pov	vy kod dostenu namietaj o zachowanju podstawov	wch zasad bezpieczeństwa:

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.



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 systemy 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

arreco

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 tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.

Numer Identyfikacyjny Wpisz numer	
DALEJ	
Pamiętaj o podstawowych zasadach bezpieczeństwa.	
Zanim wprowadzisz na stronie swój ldentyfikator użytkownika i Kod Dostępu sprawdź, czy:	
 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	
 po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę Digi/Cert 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 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:

LOGOWANIE	
Kod dostę	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 .pu .
O Par	ZALOGUJ
Zanim wpro o adres st o w pasku	wadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy: trony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) u adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
⊙ po klikn Pamiętaj: Ba Więcej infor	ięciu w kłodkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc ank nie wymaga potwierdzenia danych SMS-em lub mailem. macji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa



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

÷	Uwierzytelnianie		
		Oczekiwanie na uwierzytelnienie aplikacją mobilną Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania	

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 akceptacja autoryzacji zostaje wyswietlone 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:



÷	Uwierzytelnianie	
		Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego. Pozostań na tej stronie i potwierdz operację w aplikacji mobilnej.

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 identyfikatora alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



LOGOWANIE	PL 👻
Numer Identyfikacyjny Wpisz numer	
Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na stronie swój ldentyfikator 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 podateji Dente i uwrzesa o wiek i udodana do klik w kłodka	
rannętaj, bank ne wyniaga pouwerużenia danych swisten nou Mainem. Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa	

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:

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 Image: Construction of the state of th
	Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na stronie swój ldentyfikator użytkownika i Kod Dostępu sprawdź, czy: adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) w pasku dresu Ub 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

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

Nowe hasło dostępu			
ĺ.	 Polityka bezpieczeństwa ban 	ku wymaga zmiany hasła.	
Identyfikator użytkownika	K60001		
Nowe hasło dostępu		\checkmark	
Powtórz nowe hasło		~	
Definiując swoje no	ZAPISZ I ZALO	wau owaniu podstawowych zasad	
bezpieczeństwa:			
 musi składać si 	ę z 10-24 znaków		
o dozwolone znak XYZ!@#\$%^&*()	ki: 0123456789abcdefghijklmnopc =+{(j)\l;:",<.>/?	rstuwxyzABCDEFGHIJKLMNOPQRSTUVW	

arreco

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:

÷	Uwierzytelnianie	
		Oczekiwanie na uwierzytelnienie aplikacją mobilną Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania

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 akceptacja autoryzacji zostaje wyswietlone 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:



÷	Uwierzytelnianie	
		Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego. Pozostań na tej stronie i potwierdź operację w aplikacji mobilnej. A Błąd uwierzytelnienia WRÓĆ DO LOGOWANIA

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 tą wartość jako jednakową. Wpisywany 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 Kód 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 SIMS-em lub mailem. Wiecej informacji na ternat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa	

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:



IAWOE	١E																							
		1	2	3	4 5	6	7	8	9	10	11	12 1	3 14	15	16	17	18	19	20	21	22	23	24	
	Kod dostępu					100	•	•		•		•				•	•	•	•		•	•	•	
	Zanim wprowac	.j o po Izisz r	odstav na stro	vowyc onie si	h zasai vój Ider	dach b ntyfika	ezpiei tor uż	czeńs ytkow	twa. vnika	i Kod I	Dostę	pu spra	wdź, c	zy:										
	 adres stron 	y logo	owania	a rozp	oczyna	się od	https	(ozni	aczaja	ącego	bezp	ieczne	połącz	enie ir	terne	towe)							
	 w pasku ad 	resu li	ub na	pask	stanu	w dolr	nej cze	ęści el	kranu	przeg	glądar	ki wido	czna je	st zar	nknięt	ta kłó	odka	0						
	 po kliknięcii Pamiętaj: Bank i 	nie wy	oakę /maga	pojaw a potv	sıę cer ierdzer	tyrikat iia dar	i wyst iych S	awior MS-e	ny dia m lub	i uentr i maile	um U Im.	srug Int	ernetc	wych	przez	TITM	á niðir	uert ir	nc					
	Wienei informar	ii na t	temat	bezpi	eczeńs	twa zn	ajdzie	isz na	stror	nie: Za	sady	bezpied	zeńst	va										

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

← Uwierzyte	ianie	
	Oczekiwanie na uwierzytelnienie aplikacją mobilną Zamknięcie okna przeglądarki skutkować będzie przerwaniem procesu logowania	

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 akceptacja autoryzacji zostaje wyswietlone 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:



÷	Uwierzytelnianie	
_		Powiadomienie uwierzytelniające zostało wysłane do urządzenia mobilnego. Pozostań na tej stronie i potwierdż operację w aplikacji mobilnej.

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 włączonia usługi ASSIGN_DEVICE_WHEN_AUTHORIZE na bazie Guardiana

- 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.



De autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAR De li nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store De subrowych zasadach bezpieczeństwa: Paniętaj o podstawowych zasadach bezpieczeństwa: Sim w prowadziaz na stornie swoj lidentyfikator użytkownika i Kod Dostępu sprawdź, czy. I o sasku adresu lub na pasku staru w dolnej części ekranu przeglądsiń widocana jest zamknięta kilodka I o pasku storeju w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie w kłodką pojewi się cestyfikat wystawiony dia Centrum Usług Internetowych przez firme DigCent nic Tennet je manie nie wystawie danych SVS-em Lub maliem.	
Do autoryzacji urządzenia wymagana jest aplikacja mToken Asseco MAA Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store DOSLODM APLIKACJĘ Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na stronie swój ldentyfikator użytkownika i Kod Dostępu sprawdź, czy: o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) o adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) o pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłodka o pośkinajeciu w kłódkę pojawi się ostryfikat wystawiony da Centrum Usług Internetowych przez firmę DigiCert Inc Pamiętaj: Bank nie wymaga potwierczenia danych SMS-em lub mailem.	mToken
Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store POSIADAM APLIKACJĘ Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na stronie swój ldentyfikator 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 wriawiony dla Contrum Usług Internetowych przez firmę DigiCert Inc Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem. Wiene informaniu na temat bernierzeństwa znaktwer na stronie. Zasady bernierzeństwa	Do autoryzacji <mark>u</mark> rządzenia wymagana jest aplikacja mToken Asseco MAA
POSIADAM APLIKACUE POSIADAM APLIKACUE POSIADAM APLIKACUE Pamiętaj o podstawowych zasadach bezpieczeństwa. Zanim wprowadzisz na strónie swój ldentyfikator użytkownika i Kod Dostępu sprawdź, czy: adres stróny logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe) adres stróny 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. Wiene informanii na temat bernierzeństwa zakrieter na stronie. Zasady bernierzeństwa	Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store
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. Wiene informanii na temat bemierzeństwa znakturez na stronie. Zasady bemierzeństwa	POSIADAM APLIKACJĘ
Zanim wprowadzisz na stronie swój ldentyfikator 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 Parniętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem. 	Pamiętaj o podstawowych zasadach bezpieczeństwa.
 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. Wiane informanii na ternet bernierzeństwa znajdziesz na stronie. Zasady bernierzeństwa 	Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, ozy.
 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. Wiane informanii na ternat hemierzeństwa znajdziesz na stronie: Zasady hemierzeństwa 	 adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
 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. Wianej informanii na ternat hemierpeństwa znajdziesz na stronie: Zasady hemierzeństwa. 	 w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem. Wiana: informanii na temat hemienneństwa znajdziesz na stronie: Zasady hemienzeństwa	 po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCent Inc.
Wiene informanii na temat heznierzeństwa znajdziesz na stronie. Zasady heznierzeństwa	Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.
confinal construction of the second	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 wiażny przez 5 minut
÷	Uwierzytelnianie	
		417 985 Kod aktywacyjny Wprowadz 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.

÷	Uwierzytelnianie	
	Uwierzytelnienie poprawne.	

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

÷	Uwierzytelnianie
	×
	Wystąpił błąd Przepraszamy, napotkaliśmy błąd w obsłudze parowania
	SPRÓBUJ PONOWNIE

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 identyfikatora alfanumeryczny w polu **Numer Identyfikacyjny**. Bez względu na sposób wpisania numeru identyfikacyjnego (wielkimi czy małymi literami) system autentykacji zawsze rozpatruje tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



LOGOV	VANIE	PL
	Numer Identyfikacyjny Wpisz numer	
	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) 	
	o 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.	

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

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 • <td< th=""></td<>
	Pamiętaj o podstawowych zasadach bezpieczeństwa.
Z	anim wprowadzisz na stronie śwój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:
c	adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
c	w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
c	po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigiCert Inc
P	amiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.
V	/ęcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa

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



Nowe hasło dostępu			
	Polityka bezpieczeństwa bank	u wymaga zmiany hasła.	
ldentyfika użytkown	tor SG16ITN2G ika		
Nowe hasło doste	pu	~	
Powtorz nowe ha	sło ••••••	~	
	ZAPISZ I ZALO	am	
Definiując sv bezpieczeńs	voje nowe hasło dostępu pamiętaj o zacho twa:	waniu podstawowych zasad	
o musi sk	ładać się z 10-24 znaków		
dozwola	ne znaki: 0123456789abcdefghijkimnopqi	stuvwxyzABCDEFGHIJKLMNOPQRSTUVW	

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.

 Urządzenie autoryzujące
Do autoryzacji <mark>u</mark> rządzenia wymagana jest aplikacja mToken Asseco MAA
Jeśli nie posiadasz aplikacji, znajdziesz ją w Google Play lub App Store
POSIADAM APLIKACJĘ
D Pamiętaj o podstawowych zasadach bezpieczeństwa.
Zanim wprowadzisz na stronie swój identyfkator użytkownika i Kod Dostępu sprawdź, czy:
 adres strony logowania rozpoczyma 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 DigiCent 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	

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

÷	Uwierzytelnianie	
	Uwierzytelnienie poprawne.	

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



← Uwierzytelnianie	
×	
Wystąpił błąd	
Przepraszamy, napotkaliśmy błąd w obsłudze parowania SPRÓBUJ PONOWNIE	



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*".

OGOWANIE																						
	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														,								•
Pamięta	j o poc	dstawo	wych z	asada	ch be	zpiecze	ństwa.					02000										
Zanim wprowad	izisz ni	a stron	e swoj	Ident	ytikato	r uzytk	ownika	Kod	Dost	ępu s	praw	dz, cz	y.	*****		5						
o w pasku ad	y logov resu lu	ib na pa	ozpocz ssku st	anu w	re da r I dolne	i cześc	ekran	u prze	olada	erki wi	doczi	na ies	sue in st zan	nknie	ta kłó	idka						
o po kliknięci	u w kłó	dkę po	awi si	e certy	/fikat v	vystaw	ony dia	Cent	rum l	Jsług	Inter	netov	vych	przez	firm	ę Digi	Cert I	inc				
Pamiętaj: Bank i	nie wyr	maga p	otwien	dzenia	a dany	ch SMS	-em lui	o mail	em.				3 () -									
Wiece: informac	u no te	amat he	201607	onetu	10 700	171007	no etre	nie 7	-	have												

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

arisco



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 systemy 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 tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.



LOGOV	VANIE	PL
	Numer Identyfikacyjny SG16ITN2G	
	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). 	
	o 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 mailem.	

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:

← 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 . <td< th=""></td<>
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
 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

Po wprowadzeniu tymczasowego hasła maskowanego i wybraniu [DALEJ] podane dane są weryfikowane. Jeżeli tymczasowe hasło maskowane jest poprawne na formatce 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.

← Nowe hasło dostępu	
	Polityka bezpieczeństwa banku wymaga zmiany hasła.
identyfikator użytkownika Nowe basło dostacu	SG16ITN2G
Powtórz nowe hasło	Wpisz ponownie nowe hasło dostępu
Definiując swoje bezpieczeństwa:	ZAPISZ I ZALOGUJ nowe hasło dostępu pamiętaj o zachowaniu podstawowych zasad
o musi składać	się z 4-8 znaków
o musi zawiera	ić przynajmniej jeden znak specjalny !@#\$%^&*()=+{([]}\\;",<.>/?
 musi zawiera 	ić przynajmniej jedną wielką literę
 musi zawiera 	ić przynajmniej jedną małą literę
o musi zawiera	ić przynajmniej jedną cyfrę
dozwolone z XYZI@#\$%^8	taki: 0123456789abcdefghijklimnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVW i*0-z=+{∭\L",<>/?

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 wyswietlony 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 Kod dostępu .
Pamiętaj o podstawowych zasadach bezpieczeństwa.
Zanim wprowadzisz na stronie swój identyfikator użytkownika i Kod Dostępu sprawdż, czy:
 adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
 w pasku adresu ub na pasku stanu w dolnej częsci ekranu przeglądarki widoczna jest zamknięta kłódka
 po kunnięciu w kookę pojawi się certytikat wystawiony ola Centrum Usług internetowych przez tirmę Ligiciert inc prostaty Bryte i wystace a odwiadzania da postawa poslawi
n aniqua, bank ne mynaga powieruzenia oanych mareni.
Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa

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





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 systemy 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 tą wartość jako jednakową. Wpisywany numer identyfikacyjny jest zawsze prezentowany wielkimi literami.