SBI - CORPO

Jak się dodatkowo zabezpieczyć

Bankowość elektroniczna jest wygodną i bezpieczną formą korzystania z usług bankowych, w tym składania zleceń finansowych. W ostatnim czasie nasiliły się ataki na Klientów bankowości elektronicznej. Przestępcy nie mogąc złamać zabezpieczeń infrastruktury dostawców bankowości elektronicznej (Banków, dostawców technologii i usług), skupili się na łamaniu zabezpieczeń infrastruktury Klientów i bazowaniu na wzorcach ich zachowań. W czasach globalizacji, szalonego rozwoju usług mobilnych, coraz wyższych wymagań użytkowników co do ergonomii łatwo zapomnieć użytkownikowi o przestrzeganiu podstawowych zasad bezpieczeństwa, co przestępcy, stosując coraz bardziej wyrafinowane metody ataku, mogą wykorzystać.

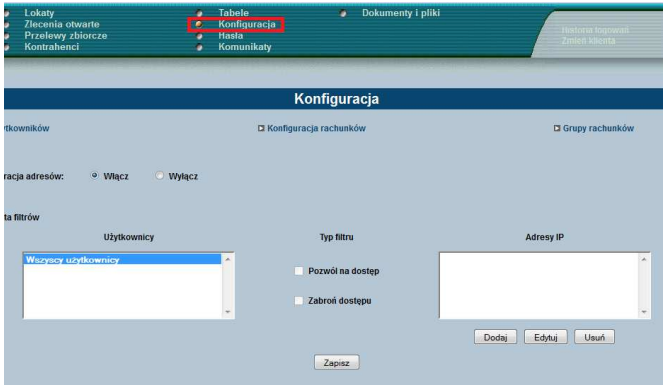
Szanowny użytkowniku, bezwzględnie stosuj się do zasad bezpieczeństwa jakie publikuje Bank, w przeciwnym razie, Twoja twierdza, jaką jest bankowość elektroniczna, ma zostawione otwarte wrota.

Bank ze swojej strony dokłada starań aby nieustannie rozwijać technologie i usługi, które będą wspierać użytkownika w wygodnym i bezpiecznym korzystaniu z bankowości elektronicznej.

Filtrowanie adresów IP.

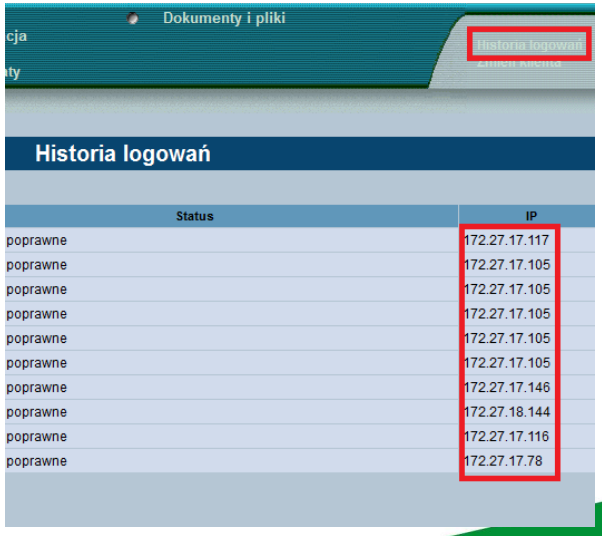
W bankowości korporacyjnej dostępne jest bardzo skuteczne narzędzie dające możliwość określenia, z jakiego adresu internetowego (IP) dozwolone jest logowanie. Funkcjonalność tą przystosowaliśmy również do tzw. dynamicznych IP poprzez możliwość definiowania klasy adresowej np. dostawcy Internetu. Filtry IP można zdefiniować na poziomie Klienta lub poszczególnych użytkowników.

Filtry IP są definiowane w opcji: Konfiguracja -> Filtry adresów IP

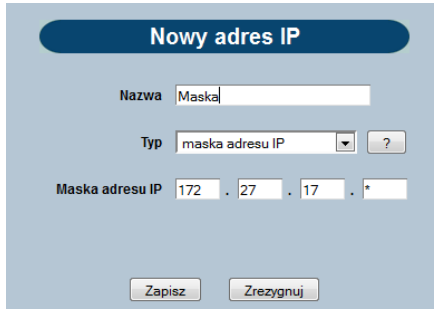


Własny adres IP można zweryfikować w opcji:

Historia logowań



W przypadku Klientów posiadających tzw. dynamiczne IP, należy na podstawie historii logowań lub po kontakcie z dostawcą Internetu ustalić odpowiednią maskę dla filtru IP. Przykładowo, z zaprezentowanego powyżej zrzutu ekranu wynika, że logowania następują z adresów IP z początkiem '172.27.17' oraz '172.27.18', zatem w takim przypadku należy zdefiniować maski '172.27.17.*' oraz '172.27.18.*'



Dodatkowo zastosowane zabezpieczenia:

Blokada edycji NRB - Funkcjonalność zabezpiecza przed podmianą numeru NRB przez osoby nieuprawnione. W przypadku konieczności zmiany przygotowanego przelewu wymagana jest dodatkowa autoryzacja. Nawet osoby, które wykradły login i hasło nie mogą ingerować w NRB na wprowadzanych przelewach.

Podpis usuwania zleceń - Zabezpieczenie chroni przed usunięciem i przygotowaniem na to miejsce „podobnego" (ze zmienionym NRB) przelewu. Wraz z blokadą edycji NRB stanowi skuteczną ochronę przed manipulowaniem NRB, przy założeniu, że osoba podpisująca przelewy weryfikuje ilość podpisywanych przelewów.

Autoryzacja dodawania/edycji szablonów/kontrahentów - Funkcjonalność zabezpiecza przed nieuprawnioną modyfikacją szablonów przelewów oraz kontrahentów. Ingerencja w listę zdefiniowanych szablonów/kontrahentów możliwa jest jedynie po dodatkowej autoryzacji.

Logowanie tokenem RSA lub VASCO - *funkcjonalność wymaga wydania tokena przez Bank dla użytkownika.*

Kod na wyświetlaczu tokena (wskazanie) zmienia się w określonych odstępach czasu.

Kontakt: tel. 75 754 67 00, e-mail: bskamgora@bskamgora.pl

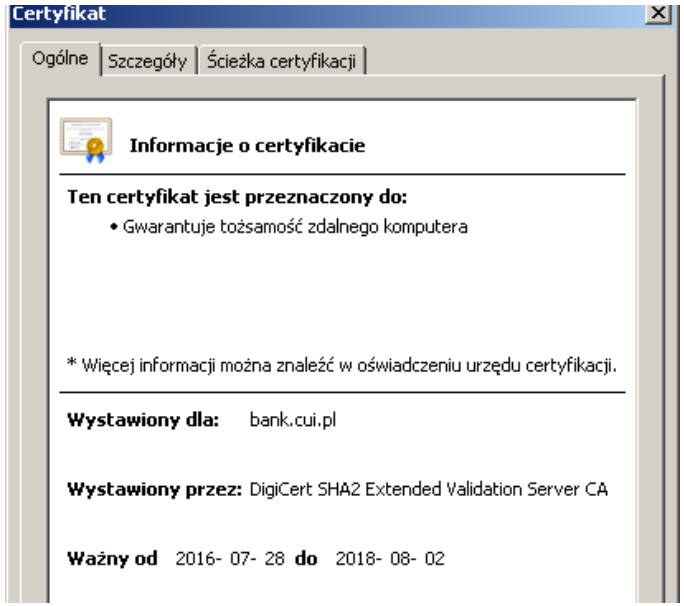
Zawsze sprawdzaj, czy certyfikat jest wystawiony przez Thawte dla bank.cui.pl klikając na kłódkę w pasku adresu

Przeglądarka Mozilla Firefox

Więcej informacji:

Przeglądarka Internet Explorer

Informacje o certyfikacie



DODATKOWE ZABEZPIECZENIA

SBI-CORPO

Przeczytaj koniecznie przed pierwszym logowaniem !!!

www.bskamgora.pl