PekaoBiznes24

Bezpieczeństwo

Wstęp

Bezpieczeństwo danych finansowych oraz transakcji przesyłanych za pośrednictwem systemu PekaoBiznes24 jest priorytetem dla Banku Pekao S.A., dlatego inwestujemy w najnowsze technologie i aktualizacje zabezpieczeń. Zapewniamy naszym Klientom najwyższy dostępny na rynku standard bezpieczeństwa, aby mogli bez obaw korzystać z naszego systemu.

Zastosowane zabezpieczenia

PekaoBiznes24 jest wyposażony w kompleksowe i spójne rozwiązania, które zapewniają użytkownikom bezpieczeństwo w każdym obszarze mającym wpływ na działanie systemu. W praktyce oznacza to:

- zabezpieczenia infrastruktury,
- zabezpieczenia organizacyjne,
- zabezpieczenia techniczne,
- bezpieczny dostęp do systemu,
- autoryzacja przesyłanych dyspozycji,
- bezpieczne technologie internetowe.

2.1 Zabezpieczenia infrastruktury

- Firewall zapewnia ochronę PekaoBiznes24 przed nieuprawnionym dostępem.
- System load balancingu, failover, klastry geograficzne zabezpieczają system przed skutkami awarii, dzięki czemu w każdej chwili mają Państwo dostęp do swoich rachunków.

- Monitorowanie aktywności użytkowników zapewnia kompleksową kontrolę działania systemu PekaoBiznes24 oraz integralności i niezaprzeczalności danych (w szczególności zleceń Klientów). Dzięki temu w pamięci programu są zapisywane wszelkie ślady aktywności użytkownika oraz wykonane operacje (np. próby logowania do systemu, odczyt historii rachunku, wykonanie przelewu itd.). Zapisywane dane obejmują również adresy IP użytkowników.

2.2 Zabezpieczenia organizacyjne

- Spójne procedury operacyjne dotyczące zarówno administratorów systemu PekaoBiznes24, jak i Doradców Klienta.
- Automatyczna blokada konta następuje w przypadku kilkukrotnego podania złych danych podczas logowania.
- Automatyczne wylogowanie odbywa się w przypadku stwierdzenia braku aktywności użytkownika w systemie w określonym czasie.

2.3 Zabezpieczenia techniczne

- Dostęp do stref technologicznych i informatycznych jest w naszym Banku ściśle kontrolowany.
- System zabezpieczeń zastosowany w Banku w pełni odpowiada światowym normom dotyczącym ochrony placówek bankowych.

2.4 Bezpieczny dostęp do systemu

Bezpieczeństwo logowania
Każda osoba uprawniona do korzystania z systemu PekaoBiznes24 otrzymuje indywidualny pakiet startowy zawierający dane niezbędne do pierwszego logowania.

Podczas pierwszego logowania system automatycznie wymusza zmianę hasła. Nowe hasło dostępu musi być zgodne z aktualną polityką bezpieczeństwa Banku, która prezentowana jest w systemie przy procesie ustalania hasła. Należy pamiętać o zapewnieniu tajności hasła i identyfikatora użytkownika, które nie powinny być znane nikomu poza jednym przypisanym użytkownikiem. Logowanie do PekaoBiznes24 możliwe jest:

- za pomocą klawiatury komputerowej,
- za pomocą klawiatury ekranowej,
- z wykorzystaniem podpisu elektronicznego na karcie procesorowej,
- z wykorzystaniem unikalnej na rynku możliwości logowania się do systemu za pomocą odcisków palców, czyli tzw. biometryka

Ograniczenie możliwości logowania
W celu zwiększenia bezpieczeństwa użytkowania systemu przez użytkowników istnieje możliwość ograniczenia możliwości logowania do systemu:

- Ograniczenie możliwości logowania użytkowników do systemu tylko ze wskazanych przez Klienta adresów IP
- Umożliwienie logowania użytkowników jedynie w określonych przez Klienta przedziałach czasowych oraz w określone dni tygodnia

Bezpieczeństwo dostępu do danych i funkcjonalności

Korzystając z PekaoBiznes24, mają Państwo możliwość ścisłego określenia uprawnień użytkowników zarówno do każdej funkcji oferowanej przez system, jak i dostępu do danych poszczególnych rachunków. Można to zrobić poprzez :

- konfigurację dostępu do danych, np.: historii operacji, salda i wyciągów,
- konfigurację dostępu do funkcjonalności, np.: wprowadzania zleceń i autoryzacji dyspozycji, prawa podpisywania i wysyłania zleceń do Banku,
- tryb super użytkownika, który pozwala na zarządzanie uprawnieniami wybranych pracowników bez potrzeby kontaktu z Bankiem (np. ograniczanie dostępu do wybranych funkcji określonym użytkownikom),
- nowoczesne systemy identyfikacji użytkowników w kontaktach z Bankiem, np. uwierzytelnianie i autoryzacja osób telefonujących na Infolinię PekaoBiznes24.

W każdej chwili mogą Państwo zmienić poszczególne uprawnienia. Wystarczy wysłać do Banku odpowiedni wniosek elektroniczny.

Bezpieczeństwo na każdym etapie procesowania płatności

- możliwość zweryfikowania osób biorących udział w tworzeniu, modyfikacji oraz autoryzacji zleceń,
- możliwość zweryfikowania osób wprowadzających i modyfikujących dane w bazie kontrahentów,
- możliwość zweryfikowania integralności importowanych plików (suma kontrolna MD5),
- możliwość importu płatności z systemu FK w postaci zaszyfrowanego pliku,
- możliwość importu płatności jako niemodyfikowalnej paczki zleceń,
- możliwość korzystania z autoryzowanej bazy kontrahentów,
- kolorowe znaczniki kontrahentów – informacja o źródłach pochodzenia kontrahenta w przelewie (kontrahent z bazy, rachunek z bazy, kontrahent i rachunek spoza bazy)
- wymuszenie weryfikacji wprowadzanego numeru rachunku w przypadku użycia metody kopiuj – wklej,
- możliwość skorzystania z rozwiązań bezpośredniej integracji systemów - wprowadzanie płatności bezpośrednio z systemu FK do systemu PekaoBiznes24,

2.5 Autoryzacja przesyłanych dyspozycji

Schematy akceptacji i limity kwotowe

System bankowości internetowej PekaoBiznes24 umożliwia konfigurację dowolnych schematów akceptacji z zachowaniem kompetencji ustalonych w firmie. Dzięki zastosowanym rozwiązaniom umożliwiamy Państwu:

- ustawienie osobnych schematów akceptacji zarówno do zleceń, wniosków, jak i przesyłanych do Banku wiadomości,
- ustawienie indywidualnych schematów akceptacji dla określonych typów transakcji,
- konfigurację schematów akceptacji do każdego z rachunków,
- weryfikację poprawności schematów,
- podgląd schematów akceptacji (w celu sprawdzenia, czy dana grupa osób może autoryzować zlecenie).

Dodatkowo system daje możliwość:

- zdefiniowania dowolnych schematów akceptacji transakcji z określeniem limitów,
- ustawienia limitów kwotowych,
- przeliczania limitów na dowolną walutę,
- ustawienia limitów terminowych, np. jednorazowych, dziennych, tygodniowych i miesięcznych sum transakcji,
- kontrolowania wykorzystania limitów - system na bieżąco kontroluje zdefiniowane limity transakcji dla każdego z rachunków osobno.

Podpis elektroniczny

W transakcjach wykonywanych za pomocą systemu PekaoBiznes24, podpis elektroniczny (zwany również podpisem cyfrowym) jest niezaprzeczalnym dowodem ich wykonania przez konkretną osobę. Podpis elektroniczny w systemie PekaoBiznes24 spełnia następujące warunki:

- identyfikuje autora podpisu,
- odróżnia ostateczne oświadczenie woli od projektów,
- umożliwia zapoznanie się z treścią dyspozycji przed jej podpisaniem,
- pozwala stwierdzić, iż oświadczenie pochodzi rzeczywiście od użytkownika, który podpisał dyspozycję przesyłaną do Banku,
- stanowi dowód, że złożone zostało oświadczenie woli o treści zamieszczonej w dyspozycji.

Główne cechy podpisu elektronicznego stosowanego w systemie PekaoBiznes24 to:

- uniemożliwia podszywanie się pod użytkownika (uwierzytelnienie osoby składającej dyspozycje),
- wykrywa wszelkie zmiany w danych transakcji (integralność transakcji),
- bezbłędnie identyfikuje autora podpisu (wiarygodność),
- blokuje osobom nieuprawnionym możliwość odczytania danych (poufność przesyłanych danych),
- wykorzystuje technologię ActiveX lub Java, dzięki której podpis elektroniczny składany jest w osobnym komponencie kryptograficznym, co dodatkowo zwiększa poziom bezpieczeństwa,
- daje możliwość obejrzenia sformatowanej i podpisanej dyspozycji,
- dzięki wykorzystaniu klawiatury ekranowej do wprowadzania hasła do klucza podpisu elektronicznego zabezpieczenia system przed przechwyceniem znaków wprowadzanych na fizycznej klawiaturze komputera, np. przez tzw. konie trojańskie.

Podpisywanie zlecenia opiera się na kluczu prywatnym dostępnym jedynie użytkownikowi oraz kluczu publicznym znajdującym się na serwerze bankowym, służącym do sprawdzania autentyczności podpisu.
Generowanie podpisu opiera się na obliczeniu sumy kontrolnej autoryzowanych danych oraz podpisaniu informacji kluczem prywatnym. Klucz prywatny może być zapisany na dowolnym nośniku (chronionym wtedy dodatkowo hasłem i kodem SMS) lub karcie procesorowej (chroniony kodem PIN i /lub odciskiem palca (identyfikatorem biometrycznym).
Użytkownik systemu PekaoBiznes24 ma możliwość korzystania z wielu kluczy podpisu elektronicznego, a także ich wyboru, ukrywania, zmiany oraz blokowania.

Certyfikaty kwalifikowane

Podobnie jak podpis elektroniczny działa wykorzystanie certyfikatów kwalifikowanych. Certyfikaty wydawane są w Polsce przez zaufane urzędy certyfikacji (Certification Authorities - CA). Certyfikat udzielany kluczowi Klienta zapewnia jego autentyczność oraz powoduje jego każdorazowe uwierzytelnienie po podpisaniu dyspozycji. Więcej na temat technologii certyfikatu kwalifikowanego znajdą Państwo na stronie www.nccert.pl.

Biometryka

Identyfikator biometryczny w postaci unikatowego odcisku palca uzupełnia dotychczasowe mechanizmy autoryzacji, takie jak hasło, PIN, karta mikroprocesorowa, klucz, token. Taki sposób identyfikacji daje gwarancję, że do systemu ma dostęp właściwy użytkownik, a nie inna osoba, która weszła w nieuprawniony sposób w posiadanie jego kodu PIN lub karty.

Sygnowanie (dodatkowe potwierdzanie)

System PekaoBiznes24 posiada dodatkową ochronę wprowadzanych, modyfikowanych i usuwanych zleceń. Funkcjonalność polega na potwierdzeniu przez użytkownika poprawności wprowadzanych zmian lub woli wykonania danej czynności z wykorzystaniem podpisu elektronicznego lub jednorazowego kodu SMS

2.6 Bezpieczne technologie internetowe

Bezpieczna komunikacja z Bankiem poprzez system PekaoBiznes24 zapewniona jest dzięki:

- certyfikacji WEB serwerów przez zaufane centrum autoryzacji,
- wykorzystaniu technologii szyfrowania TLS z kluczem o długości 128 bitów,
- zabezpieczeniu przesyłanych danych przed manipulacją lub utratą,
- kontroli aktywności w systemie poprzez zastosowanie jednoseryjnych kluczy,
- logom systemowym – rejestrze wszystkich aktywności użytkowników i systemu.

Protokół kryptograficzny SSL (Secure Socket Layer) wykorzystywany w systemie PekaoBiznes24 korzysta z dwóch metod kryptografii: metody HYPERLINK, czyli klucza publicznego oraz szyfrowania symetrycznego.

W przeglądarkach internetowych Internet Explorer, Mozilla oraz Netscape nawiązanie bezpiecznego połączenia sygnalizowanie jest pojawieniem się ikony zamkniętej kłódki w prawym dolnym rogu ekranu. TLS korzysta z tzw. certyfikatów autentyczności wystawianych instytucjom przez powołane do tego niezależne urzędy Certification Authorities (CA). Certyfikat Banku zawiera jego klucz publiczny. Dzięki autoryzacji możemy być pewni, że należy on do Banku Pekao S.A.
W pierwszej fazie nawiązywania połączenia TLS serwer i przeglądarka wymieniają certyfikaty, czyli odpowiedniki dokumentu tożsamości Państwa i serwera WWW. Ważną sprawą dla bezpieczeństwa zaszyfrowanych informacji jest długość używanych kluczy.

- W systemie PekaoBiznes24 wynosi on 128 bitów.
- Im dłuższe są klucze, tym trudniej jest odszyfrować informacje.
- Stosowanie dla kluczy symetrycznych 128 bitów zapewnia wysoki poziom bezpieczeństwa.

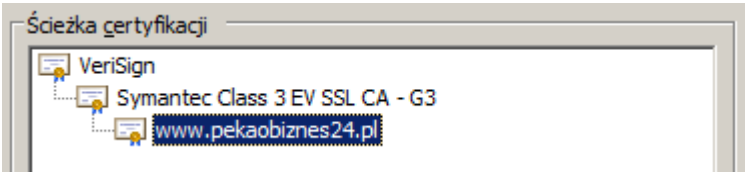
Zasady zachowania bezpieczeństwa

PekaoBiznes24 to bezpieczny system bankowości internetowej dla korporacji. Unikalne, dopasowane do potrzeb przedsiębiorstwa mechanizmy bezpieczeństwa dają najwyższy poziom ochrony przy wymianie danych między systemami finansowo-księgowymi i PekaoBiznes24. Pamiętajmy jednak, że bezpieczeństwo realizowanych operacji zależy również od postępowania użytkowników. Nasz poradnik pomoże Państwu zachować ostrożność podczas korzystania z systemu oraz innych narzędzi online. Oto proste zasady, o których zawsze warto pamiętać:

- należy się logować do systemu bezpośredniego pod adresem https://www.PekaoBiznes24.pl lub ze strony głównej Bankowości Korporacyjnej Banku – http://www.korporacje.pekao.com.pl
- nie należy uruchamiać systemu, korzystając z załączników lub linków otrzymanych pocztą e-mail oraz linków, niezlokalizowanych na stronach Banku.
- nie należy odpowiadać na e-maile z prośbą o weryfikację danych użytkownika, a w szczególności przesyłać pocztą elektroniczną swoich danych identyfikacyjnych, takich jak dane osobowe, login, hasło, dane rachunku bankowego czy numer karty kredytowej.
- nie należy otwierać załączników otrzymanych pocztą e-mail od nieznanych nadawców lub wraz z wiadomością o podejrzanej treści – takie załączniki to zwykle skompresowane wirusy i konie trojańskie, których celem jest pozyskanie dostępu do komputera i poufnych danych użytkownika, tj. login, hasła, klucze, piny
- warto unikać logowania się do systemu bankowości internetowej z komputerów, do których nie ma się pełnego zaufania (np. w kawiarenkach internetowych),
- trzeba pamiętać o zabezpieczeniu komputera, z którego wykonywane są operacje bankowości internetowej:
  - należy instalować tylko legalne oprogramowanie oraz wszystkie poprawki zalecane przez producenta,
  - należy zainstalować i używać oprogramowanie antywirusowego:

- warto stosować ochronę w czasie rzeczywistym,
- nie należy zapominać o regularnej aktualizacji bazy danych wirusów oraz regularnym skanowaniu komputera.

- podczas procesu logowania koniecznie należy sprawdzić, czy strona podpisana jest aktualnym certyfikatem wystawionym przez zaufane centrum certyfikacji (trzeba dwukrotnie kliknąć lewym klawiszem myszy na ikonę kłódki znajdującą się w prawym dolnym rogu okna przeglądarki – otworzy się okno z właściwościami certyfikatu). Certyfikat bezpieczeństwa należy zweryfikować według następujących kryteriów:
  - dla kogo został wystawiony certyfikat: www.pekaobiznes24.pl,
  - aktualna data ważności certyfikatu,
  - kto wystawił certyfikat, (aktualny certyfikat wystawiło dla Banku centrum certyfikacji VeriSign),
  - jaka jest ścieżka certyfikacji (obecna ścieżka ważna do 10.04.2017 r)



  Po prawidłowym zweryfikowaniu Certyfikatu można bezpiecznie kontynuować logowanie do systemu.
- podczas logowania wciśnięcie symbolu  pozwala uzyskać dostęp do tzw. wirtualnej klawiatury. Wykorzystanie tej funkcji ogranicza ryzyko poznania hasła przez osoby niepowołane.
- po zakończeniu korzystania z platformy transakcyjnej należy wylogować się z systemu.
- nie wolno ujawniać nikomu swoich identyfikatorów i haseł, zapisywać tych danych i przechowywać w pobliżu komputera.
- po podpisaniu zleceń kluczem zapisanym na karcie kryptograficznej lub urządzeniu integrującym kartę i czytnik (token) należy wyciągnąć kartę z czytnika lub wyjąć token z portu USB,
- należy chronić swój telefon komórkowy przed dostępem niepowołanych osób i instalacją złośliwego oprogramowania. Szczególnie kiedy odbierane są na nim smsy z kodem dobezpieczającym proces podpisywania zleceń z użyciem klucza zapisanego na nośniku lokalnym.

Kontakt

W przypadku dodatkowych pytań prosimy o kontakt z Infolinią PekaoBiznes24

- Mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa:
  pb24@pekao.com.pl
  22 59 12 323
- Duże firmy i korporacje:
  pekaobiznes24@pekao.com.pl
  22 59 12 222