



PAKIET DLA ADMINISTRACJI

ePODATKI

INFORMACJE WYMIAROWE PRZEZ INTERNET

Usługi Informatyczne INFO-SYSTEM, Roman i Tadeusz Groszek s.j.

05-120 Legionowo, ul. Piłsudskiego 31/240, tel. 0 22 784 49 44, fax 0 22 784 49 88, www.groszek.pl, e-mail: poczta@groszek.pl

NIP: 5361745379, REGON: 015664091, KRS: 0000296313

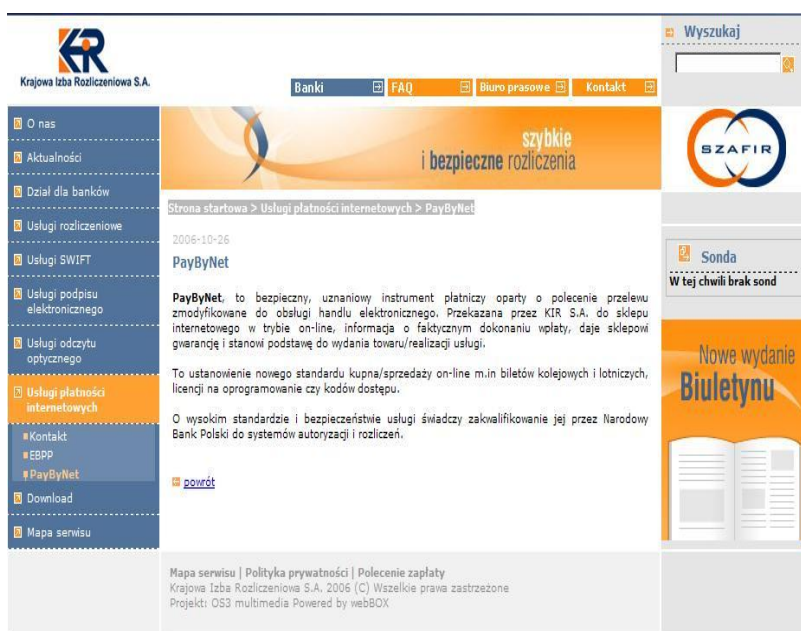
SPIS TREŚCI

Wstęp	3
Opis funkcjonalny	3
Wykorzystanie usługi przez podatnika	3
PayByNet.....	4
Wykorzystanie usługi w połączeniu z UPK.....	4
Sposoby wykorzystania systemu.....	5
Korzyści.....	6
Nadawanie i kontrola uprawnień	6
Wymagania	6
Zgodność z przepisami	7
Opis techniczny	7
Wykorzystywane technologie.....	7
Moduły	7
Schemat powiązań w ramach systemu ePodatki.....	8
Usługa sieciowa <i>ServInfoSysAP</i>	8
Założenia techniczne dotyczące komunikacji pomiędzy serwerem aplikacji a usługą sieciową <i>ServInfoSysAP</i>	10
Integracja modułów ePodatki	11
Bezpieczeństwo	12

Po zrealizowaniu płatności urząd otrzymuje wyciąg bankowy, który jest wczytywany przez specjalny program – analiza operacji wykonanych przez *Internet* pozwala na automatyczne zaksięgowanie wpłat na poczet należności i odsetek na podstawie szczegółowych informacji, zgromadzonych podczas realizowania płatności przez użytkownika.

PAYBYNET

Usługa *PayByNet*, autorstwa Krajowej Izby Rozliczeniowej, to bezpieczny, uznaniowy instrument płatniczy oparty o polecenie przelewu zmodyfikowane do obsługi handlu elektronicznego. O wysokim standardzie i bezpieczeństwie usługi świadczy zakwalifikowanie jej 31 stycznia 2006 r. przez Narodowy Bank Polski do systemów autoryzacji i rozliczeń oraz wyrażenie zgody na prowadzenie tego systemu przez KIR S.A.



Krajowa Izba Rozliczeniowa jest nowoczesną, solidną i godną zaufania instytucją, która od lat zajmuje uznaną i stabilną pozycję w polskim systemie bankowym. Realizując swoje zadania statutowe KIR S.A. prowadzi obsługę zleceń płatniczych wyłącznie poprzez elektroniczne systemy rozliczeń międzybankowych (ELIXIR).

WYKORZYSTANIE USŁUGI W POŁĄCZENIU Z UPK

UPK - Uniwersalny Program Księgujący

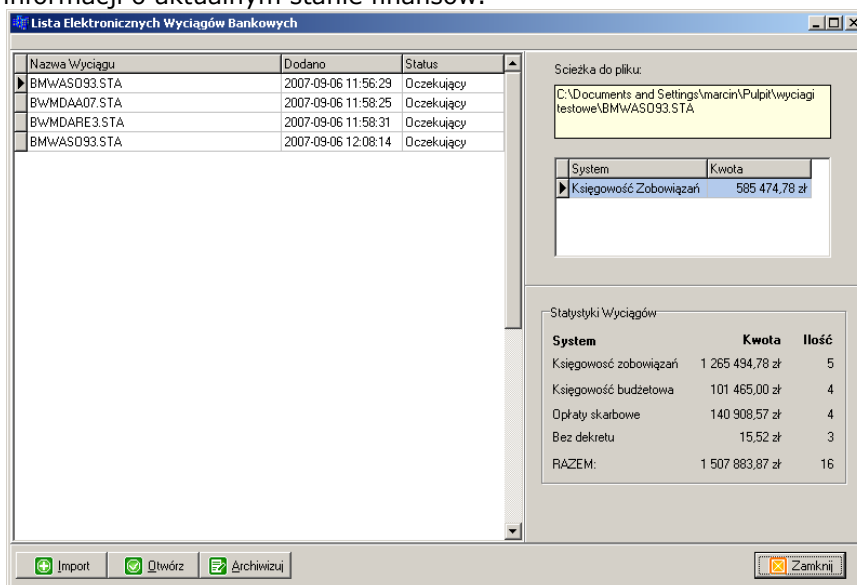
Nowa aplikacja pozwala na znaczne przyspieszenie i zautomatyzowanie rejestrowania operacji finansowych, otrzymywanych na wyciągach bankowych:

1. Wyciągi bankowe przekazywane w postaci plików (dyskietka, mail, usługa sieciowa) są wczytywane przez program, dzielone na poszczególne operacje i analizowane;
2. W **najprostszym przypadku** to operator decyduje, gdzie należy zarejestrować operację: w systemie księgowości budżetowej, na koncie analitycznym podatnika, w rejestrze opłat skarbowych;
3. Przy **wykorzystaniu wirtualnych kont bankowych** program automatycznie rozpoznaje, na jakim koncie i w ramach jakiego zobowiązania należy wykonać księgowanie;
4. W połączeniu z modułem **płatności elektronicznych** program automatycznie wykonuje księgowanie – łącznie z podziałem wpłaconej kwoty na należne raty, wraz z wydzieleniem kwot odsetek;
5. Jednocześnie z programu może korzystać wielu operatorów;
6. Można pracować nad wieloma wyciągami na raz;

Usługi Informatyczne INFO-SYSTEM, Roman i Tadeusz Groszek s.j.

05-120 Legionowo, ul. Piłsudskiego 31/240, tel. 0 22 784 49 44, fax 0 22 784 49 88, www.groszek.pl, e-mail: poczta@groszek.pl
NIP: 5361745379, REGON: 015664091, KRS: 0000296313

7. Nie ma już więcej konieczności ręcznego przepisywania informacji z wyciągu – wszystkie dane opisowe oraz kwoty są przenoszone do księgowania automatycznie;
8. Szerokie możliwości raportowania zapewniają pełną kontrolę nad pracą, wykonywaną przez różne osoby w ramach dowolnej liczby wyciągów i operacji księgowych;
9. Przetworzenie wyciągów z wykorzystaniem programu pozwala na szybszy i pełniejszy dostęp do informacji o aktualnym stanie finansów.



SPOSOBY WYKORZYSTANIA SYSTEMU

Wersja	Komponenty
Wersja informacyjna Umożliwia podgląd informacji o danych wymiarowych i bieżących należnościach wraz z odsetkami.	1. Rejestr użytkowników; 2. Usługa sieciowa (odczyt danych); 3. Serwer aplikacji (realizowany lokalnie w urzędzie lub w ramach usługi hostingowej);
Wersja pełna Umożliwia wybór należności i zrealizowanie płatności poprzez system <i>PayByNet</i> (KIR).	4. Dodatkowa usługa sieciowa (zapis sesji); 5. Rejestr sesji;
Wersja rozszerzona Pozwala na automatyczne zapisywanie na kontach podatników wpłat, wniesionych poprzez Internet.	6. Uniwersalny Program Księgujący.

KORZYŚCI

1. **Bezpośredni dostęp do informacji wymiarowej** - dla wszystkich zainteresowanych osób fizycznych i prawnych, łącznie z rozliczeniami księgowymi; pracownicy są odciążeni od udzielania szczegółowych informacji podatnikom;
2. **Ułatwienie dla podatników** – opłat można dokonywać z dowolnego komputera – w pracy, w domu, w kiosku informacyjnym na terenie gminy, w dowolnym czasie, bez konieczności oczekiwania;
3. **Lepsza ściągalność należności** – podatnik ma kompletną informację o swoim stanie rozliczeń, wpłaty na poczet należności są dokonywane łącznie z odpowiednimi odsetkami, ponadto wpłaty rozksięgowywane są na należność i odsetki;
4. **Ułatwienie w księgowaniu** – wyciągi w postaci elektronicznej mogą być rejestrowane na kontach podatników z minimalnym udziałem operatora;
5. **Doskonale uzupełnienie projektów e-Gmina/e-Społeczeństwo** – urząd świadczy usługi internetowe w pełnym wymiarze.

NADAWANIE I KONTROLA UPRAWNIEŃ

Uwierzytelnianie

Chętni do skorzystania z usług internetowego podglądu swoich zobowiązań podatkowych powinni zwrócić się do urzędu, wypełniając formularz rejestracyjny na stronie internetowej urzędu. Dane są weryfikowane przez urzędnika (może być konieczne ujednolicenie wpisów o danym podatniku, wypełnienie brakujących danych, itp.). Na podstawie złożonego formularza podatnicy są rejestrowani jako użytkownicy w systemie, mając nadana nazwę (login) i hasło. Do pełnej weryfikacji może być potrzebne wezwanie użytkownika z dowodem tożsamości do urzędu. Dane zarejestrowanych użytkowników są przechowywane w bazie danych w urzędzie. Po wejściu na stronę internetową konieczne jest przedstawienie się usłudze - podanie nazwy i hasła, które są przekazywane do usługi sieciowej, weryfikującej ich poprawność.

Autoryzacja

Po zalogowaniu się użytkownik posiada dostęp tylko do tych danych wymiarowych i związanych z nimi rozliczeń księgowych, które jego bezpośrednio dotyczą.

WYMAGANIA

Sprzęt i konieczne oprogramowanie:

1. Baza danych – na serwerze Windows/Linux;
2. Usługa sieciowa – Wydzielony komputer w Windows i IIS, zabezpieczony przed dostępem z zewnątrz, z bezpiecznym połączeniem z bazą danych;

Przygotowanie danych:

3. Uzupełnianie numerów PESEL/NIP dla osób, korzystających z e-Podatków – szukanie po nazwisku jest mało efektywne i niejednoznaczne;
4. Porządkowanie baz podatkowych – ujednolicanie wpisów dotyczących podatników (każda osoba wprowadzona jeden raz).

ZGODNOŚĆ Z PRZEPISAMI

Usługa ePodatki jest zgodna z ROZPORZĄDZENIEM RADY MINISTRÓW z dnia 11 października 2005r. **w sprawie minimalnych wymagań dla systemów teleinformatycznych.**

OPIS TECHNICZNY

WYKORZYSTYWANE TECHNOLOGIE

WebService

Komponent programowy udostępniający usługi przez sieć, używający do komunikacji protokołu [SOAP](#), nazywany też usługą sieciową.

Aplikacja

Element oprogramowania użytkowego, udostępniający funkcjonalność pozwalającą na realizację konkretnych zadań. Aplikacja internetowa jest zasobem pozwalającym wzbogacić serwisy internetowe, współpracującym głównie z bazami danych.

WebBroker

Technologia oprogramowania służąca do budowy serwisów internetowych. Przy jej pomocy można integrować się z różnymi usługami sieciowymi, tworząc konkretną aplikację internetową.

MODUŁY

BOAdmin

Aplikacja rejestrująca użytkowników.

ePodatki serwer usług sieciowych ServInfoSysAP

Zestaw usług sieciowych, zapewniających komunikację z bazą danych, uwierzytelnianie i autoryzację użytkowników, odczyt danych, zapis i potwierdzanie sesji płatności internetowych. Usługi działają w siedzibie urzędu.

ePodatki serwer aplikacji

Aplikacja umożliwiająca prezentację danych podatkowych i zapewniająca interakcję z użytkownikiem. Aplikacja jest realizowana w oparciu o serwer JBoss, dostępny na zasadzie OpenSource, może być uruchamiana w siedzibie urzędu lub u dostawcy usług hostingowych.

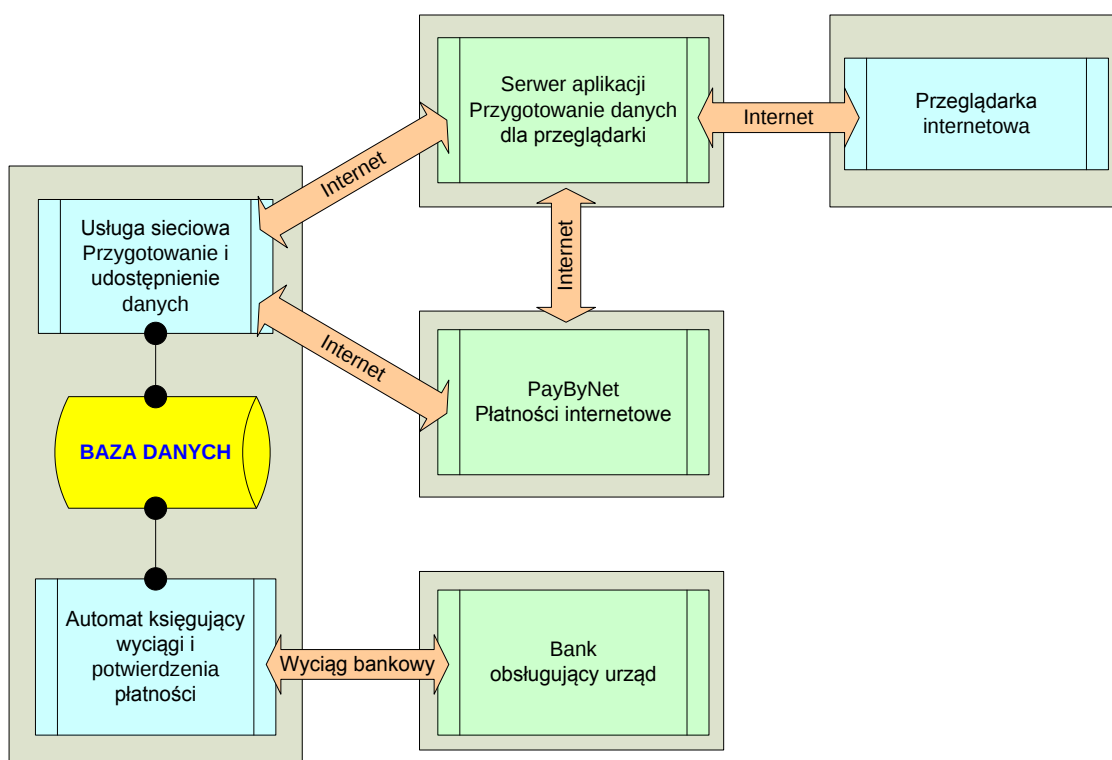
PayByNet

System płatności internetowych autorstwa Krajowej Izby Rozliczeniowej.

UPK

Program odczytujący i księgujący elektroniczne wyciągi bankowe.

SCHEMAT POWIĄZAŃ W RAMACH SYSTEMU EPODATKI



USŁUGA SIECIOWA SERVINFOSYSAP

Opis

Usługa sieciowa *ServInfoSysAP* udostępnia następujące funkcjonalności:

1. Rejestrowanie zgłoszeń osób, które chcą uzyskać dostęp do danych ich dotyczących zgromadzonych w bazie *Pakietu dla Administracji*;
2. Zwracanie informacji o danych zgromadzonych w bazie *Pakietu dla Administracji* na temat danej osoby, po jej uprzednim uwierzytelnieniu i autoryzacji.

Wymagania

Usługa sieciowa działa jako aplikacja CGI (komunikacja z serwerem aplikacyjnym poprzez strumień wejścia i wyjścia) pod nadzorem systemu *Windows*. Wymaga zainstalowania serwera internetowych usług informacyjnych *IIS* (ze względów bezpieczeństwa powinna to być wersja co najmniej 6.0) i udostępnienia usług: *Publikowanie w sieci WWW* i *Administrator programu IIS*.

Katalog, w którym aplikacja jest zainstalowana, musi być udostępniony w sieci Web. W *Uprawnieniach dostępu* należy zaznaczyć *Odczyt*, a w *Uprawnieniach aplikacji* należy wybrać *Wykonaj (łączenie ze skryptami)*.

Instalacja

Instalowanie aplikacji implementującej usługę sieciową wykonuje się za pomocą dedykowanego programu instalacyjnego. Instalator wgrywa do wskazanego katalogu aplikację *ServInfoSysAP.exe* wraz z częścią bibliotek i plików pomocniczych. Pozostałe biblioteki wgrywane są do podkatalogu *SYSTEM32*, znajdującym się w katalogu systemowym (zwykle o nazwie *WINDOWS*).

Program *ServInfoSysAP* po uruchomieniu go przez serwer nawiązuje połączenie z bazą danych. Informacja o jej położeniu odczytywana jest z pliku konfiguracyjnego *ServInfoSys.xml* (plik ma strukturę taką samą, jaka jest używana we wszystkich aplikacjach z *Pakietu dla Administracji*; edycję tego pliku można przeprowadzać za pomocą programu *Admin3*).

Zalecane jest, aby dostęp do bazy danych odbywał się poprzez protokół TCP/IP. W tym celu wystarczy do pliku konfiguracyjnego wpisać położenie bazy danych przy użyciu adresu IP.

Po zainstalowaniu aplikacji należy pamiętać o udostępnieniu w sieci Web katalogu, w którym aplikacja się znajduje.

Zasady korzystania z usługi sieciowej ServInfoSysAP

Usługa sieciowa *ServInfoSysAP* udostępnia kilka funkcji. Korzystając z danej funkcji należy pamiętać, że w przypadku wystąpienia błędów, które nie pozwalają na jej prawidłowe zakończenie, zostanie zgłoszony wyjątek typu *EServInfoSysAPExc*. Wyjątek ten należy przechwycić po stronie klienta wywołującego usługę sieciową. Opis błędu zawiera właściwość *Message*. Same błędy mogą być spowodowane niewłaściwą konfiguracją usługi (np. brak dostępu do bazy danych), nieprawidłową zawartością danych przesłanych do usługi, błędami w kodzie aplikacji.

Dane wysyłane do usługi

Dane wysyłane do usługi przez klienta z niej korzystającego muszą spełniać następujące warunki:

1. Być dokumentem XML zgodnym ze schematem opisującym argument wywoływanej funkcji,
2. Dokument musi być zaszyfrowany za pomocą algorytmu opisanego w dokumencie XML zwracanym przez funkcję *pobierzDaneKonfiguracyjne()*;
3. Zaszyfrowany dokument musi zostać przekształcony do postaci *Base64*.

Podsumowując można powiedzieć, że dane wysyłane do usługi są zaszyfrowanymi dokumentami *XML* spełniającymi dedykowany schemat (*XML Schema*), przy czym szyfrogram jest zapisany w postaci *Base64*.

Funkcja pobierzDaneKonfiguracyjne()

Deklaracja

```
string pobierzDaneKonfiguracyjne()
```

Opis

Funkcja zwraca informacje o danych konfiguracyjnych usługi sieciowej. Zwracany łańcuch znaków jest dokumentem *XML* zakodowanym do postaci *Base64*. Struktura i treść dokumentu opisane są poprzez *XML Schema* zawarty w pliku *konfiguracja.xsd*. Dokument m.in. niesie informacje o algorytmie szyfrującym, który powinien być używany do zaszyfrowania danych wysyłanych do usługi.

Funkcja rejestrujZgloszenie()

Deklaracja

```
int rejestrujZgloszenie(string formularz)
```

Opis

Zadaniem funkcji jest zarejestrowanie w bazie danych zgłoszenia, dzięki któremu dana osoba może dostać uprawnienia do dostępu poprzez *Internet* do danych jej dotyczących.

Formularz przekazany w wywołaniu funkcji musi spełniać warunki podane w rozdziale *Dane wysyłane do usługi* oraz być zgodny ze schematem zawartym w pliku *form-zgl.xsd*.

Funkcja zwraca liczbę całkowitą o następujących wartościach: 0 (zero) – gdy zgłoszenie zostanie zarejestrowane, 1 (jeden) – gdy w bazie danych znajduje się już zgłoszenie od osoby o tej samej nazwie logowania.

Funkcja pobierzDaneUzytkownika()

Deklaracja

```
string pobierzDaneUzytkownika(string login_info)
```

Opis

Funkcja służy do zalogowania użytkownika opisanego za pomocą argumentu *login_info* i zwrócenia informacji o danych jego dotyczących. Informacje zwracane są pod warunkiem udanego zalogowania.

Informacje dotyczące logującego się użytkownika przekazane za pomocą argumentu *login_info* muszą spełniać warunki podane w rozdziale *Dane wysyłane do usługi* oraz być zgodne ze schematem zawartym w pliku *login-info.xsd*.

Odpowiedź zwracana przez funkcję jest dokumentem XML zgodnym ze schematem zawartym w pliku *uzytkownik-info.xsd*. Sam dokument jest zaszyfrowany za pomocą algorytmu i klucza przekazanego w argumencie *login_info* i przekształcony do postaci *Base64*.

W przypadku nieudanego zalogowania użytkownika, którego przyczyną jest niepoprawna nazwa lub hasło, funkcja zgłasza wyjątek. Tak samo traktowany jest przypadek, gdy nazwa i hasło jest poprawne, ale procedura przetworzenia zgłoszenia nie dobiegła końca. Oba przypadki różnią się oczywiście opisem, który niesie w sobie wyjątek.

ZAŁOŻENIA TECHNICZNE DOTYCZĄCE KOMUNIKACJI POMIĘDZY SERWEREM APLIKACJI A USŁUGĄ SIECIOWĄ SERVINFOSYSAP

Dokumenty XML, które otrzymują i zwracają usługi sieciowe są ściśle zdefiniowane oraz szyfrowane i zapisywane w formacie *Base64*.

Usługa dostarcza informacji konfiguracyjnych:

1. Klucz publiczny;
2. Numer wersji;
3. Nazwa algorytmu do szyfrowania z numerem wersji;
4. Nazwa algorytmu do obliczania skrótu.

Hasło użytkownika przesyłane jest w postaci skrótu obliczanego algorytmem z punktu powyższego. Wszystkie dane binarne wewnątrz XML-a są zapisywane w formacie *Base64*.

Rejestrowanie użytkownika

1. Formularz konwertowany do XML i wysyłany za pomocą dedykowanej usługi sieciowej z dołączonym kluczem publicznym wysyłającego wraz z nazwą algorytmu i numerem wersji;
2. Szyfrowany za pomocą klucza publicznego i algorytmu (opisane powyżej);
3. Zwrotnie wysyłane jest informacja o powodzeniu lub opis błędu (też XML);

Logowanie

4. Do usługi przekazywane są: nazwa użytkownika, skrót hasła, adres IP, data (z czasem), klucz publiczny wywołującego usługę;
5. Zwrotnie wysyłany jest dokument XML z informacją o powodzeniu logowania, a w przypadku błędu jego opis;
6. W przypadku udanego zalogowania zwracana jest pełna informacja o danych zalogowanego użytkownika;

Zapisywanie płatności wybranych przez użytkownika

7. Dokument musi zawierać nazwę użytkownika i jego hasło (skrót);
8. Cała operacja realizowana jest w trzech krokach:
 - a. Powiadomienie (za pomocą dedykowanej usługi sieciowej) o przystąpieniu do realizacji płatności; zwrotnie wysyłana jest informacja o powodzeniu; w przypadku błędu (zwracany jest jego opis) przerywamy operację;
 - b. Przekierowanie do KIR-u z podaniem płatności do zrealizowania; zwrotnie wysyłana jest informacja o powodzeniu lub błędzie;
 - c. Powiadomienie (za pomocą dedykowanej usługi sieciowej) o stanie zrealizowania płatności przez KIR (powodzenie lub błąd).

INTEGRACJA MODUŁÓW EPODATKI

Połączenie	Sposób połączenia
Użytkownik – – Serwer aplikacji	Generowana jest strona HTML z apletem języka Java, który przy pomocy połączenia SSL komunikuje się z serwerem aplikacji.
Serwer aplikacji – – Serwer usług sieciowych	Połączenie poprzez firewall. Przesyłane pakiety informacji są dodatkowo szyfrowane za pomocą algorytmu RSA o sile 1024, 2048, 4096 bitów , w zależności od ustawień systemu.
Serwer usług sieciowych – – Baza danych	Odpowiednia konfiguracja dostępu do bazy danych uniemożliwia dostęp z zewnątrz.
PayByNet	Podpis elektroniczny, biblioteka kryptograficzna, SSL W ramach systemu PayByNet w komunikacji między użytkownikami i modułami systemu PayByNet stosowane są połączenia SSL szyfrowane kluczem o długości 128 bitów. Podczas połączenia następuje jednostronne uwierzytelnienie ze strony serwera WWW obsługującego system PayByNet.

BEZPIECZEŃSTWO

Usługa sieciowa *ServInfoSysAP* wymaga, aby dane przekazywane między usługą, a klientem były szyfrowane za pomocą algorytmu RSA. W przypadku danych wejściowych używany jest klucz publiczny dostarczany przez samą usługę za pomocą dedykowanej funkcji. Do zaszyfrowania danych wyjściowych używany jest z kolei klucz publiczny dostarczony przez klienta wywołującego usługę.

Aby klient mógł otrzymać dane wymiarowe pobierane z bazy danych urzędu konieczne jest jego uwierzytelnienie i autoryzacja. Uwierzytelnienie odbywa się przez podanie nazwy (login) oraz hasła (dane te przed wysłaniem muszą zostać zaszyfrowane za pomocą klucza publicznego usługi sieciowej). Autoryzacja ma na celu określenie zakresu danych, które mogą zostać zwrócone klientowi. Sam zakres danych ustalany jest przez pracownika urzędu podczas rejestrowania zgłoszenia od klienta.

Bezpieczeństwo aplikacji internetowej zależy w dużej mierze od technologii użytej do jej budowy. Nasz produkt jest wykonywalnym programem i w odróżnieniu od innych aplikacji internetowych nie jest oparty na języku skryptowym. Do użytkownika wysyłany jest program binarny znajdujący się w jednym pliku (archiwum jar). Wszystkie dane, na których program operuje znajdują się w specjalnie zabezpieczonym miejscu w pamięci RAM (Sun Microsystems Java security box - Sandbox). Program nie ma fizycznej możliwości zapisu jakichkolwiek danych na dysku komputera. Komunikacja pomiędzy programem uruchomionym w przeglądarce a serwerem JBoss również została zabezpieczona. Na potrzeby komunikacji program generuje mocny klucz RSA (o długości 2048 bitów). Tak zabezpieczone wiadomości są bardzo trudne do odszyfrowania. Dodatkowo każda wiadomość zawierająca dane użytkownika podpisywana jest specjalnym kodem, który gwarantuje, że mogła ona zostać wygenerowana tylko przez aplikację ePodatki. Inne programy nie mogą poprawnie odczytywać, czy ingerować w tak zabezpieczone komunikaty. System cyfrowo podpisywanych komunikatów zabezpiecza przed atakami na sesję komunikacyjną, dzięki czemu nie istnieje możliwość podszycia się pod poprawnie zalogowanego użytkownika, czy wykonanie zapytania SQL.

Usługa znajdująca się po stronie serwera JBoss również musi zostać zabezpieczona. Jest ona najczęściej narażony na ataki. Usługa serwisu ePodatki nie posiada bezpośredniego dostępu do bazy danych. Informacje dostarczane do użytkownika odczytuje z usługi sieciowej zainstalowanej na serwerze IIS. Komunikaty wysyłane pomiędzy serwerami są szyfrowane.

Usługa ePodatki oczekuje na zaszyfrowany i podpisany komunikat wysłany przez Aplikację z przeglądarki klienta. Zawiera ona interfejs funkcji, które może wykonać usługa sieciowa. Kiedy komunikat nie zostałby podpisany (jego podpis nie jest zgodny z podpisem aplikacji ePodatki), lub gdy próbuje on wykonać niedozwoloną operację następuje przerwanie programu. Nie można wygenerować komunikatu, który wykonywałby dowolne zapytanie w bazie danych. Odczyt informacji z przechwyconych komunikatów nie jest możliwy. Wszystkie informacje są szyfrowane jednorazowym kluczem RSA, który po wylogowaniu użytkownika zostaje bezpowrotnie wymazany z pamięci komputera.