Krajowa Izba Rozliczeniowa S.A.

PayByNet

Specyfikacja interfejsów dla Sklepów

Warszawa – czerwiec 2012

Spis treści

Zastosowanie Unified Modeling Language

Zachowanie systemu, sposób współpracy elementów systemu, fizyczne komponenty systemu oraz ich styk z wykorzystywaną infrastrukturą sprzętową opisano przy pomocy języka UML:

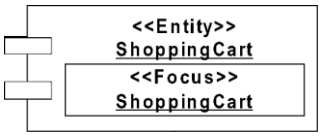
- zachowanie systemu oraz oczekiwane efekty działania systemu opisano przy użyciu diagramów przypadków użycia,
- sposób współpracy elementów systemu opisano przy użyciu diagramów przebiegu, kooperacji, stanów i czynności,
- podział systemu na komponenty – fizyczne, wymienne części, wykorzystujące i realizujące pewne zbiory interfejsów – zobrazowano przy użyciu diagramów komponentów,
- fizyczne aspekty wdrożenia systemu, a w szczególności styk komponentów systemu i jego infrastruktury sprzętowej opisano przy użyciu diagramów wdrożenia.

Dostępność

System PayByNet działa 24/7/365 w warunkach jednoczesnego przetwarzania w dwóch, fizycznie oddalonych od siebie na odległość kilku kilometrów, ośrodków obliczeniowych KIR S.A. W ramach systemu istnieją mechanizmy pozwalające na: jednoczesną pracę elementów systemu w dwóch, oddalonych od siebie ośrodkach obliczeniowych Izby, przejęcie całości obciążenia systemu przez elementy systemu znajdujące się w jednym z ośrodków Izby na wypadek awarii elementów znajdujących się w drugim z ośrodków oraz powrót do normalnej pracy po usunięciu awarii, odtworzenie, w przypadku poważnej awarii, systemu w jednym lub obu ośrodkach Izby.

Informacje prawne

Konwencje typograficzne

czcionka wytłuszczona	Używana jest w celu oznaczenia: • nazwy poleceń, opcji, słów kluczowych, nazwy skryptów (gdy omawiane są jako polecenia, a nie jako pliki) • wywołań funkcji systemowych, programów narzędziowych
czcionka pochylona	Używana jest w celu oznaczenia: • ścieżek dostępu, nazwy plików, użytkowników, grup • parametrów systemowych, zmiennych środowiskowych, atrybutów obiektów i słów kluczowych zawartych w tekście dokumentacji w tekście dokumentacji, • pakietów oprogramowania, • nowych terminów i pojęć gdy pojawiają się po raz pierwszy, • komentarzy umieszczonych wśród zawartości plików
czcionka o stałej szerokości	Używana jest w celu oznaczenia: • zawartości plików, • komunikatów wyświetlanych przez polecenia
wytłuszczona czcionka o stałej szerokości	Używana jest w celu oznaczenia poleceń lub innego tekstu wpisywanego przez użytkownika
pochylona czcionka o stałej szerokości	Używana jest w celu oznaczenia tekstu, który powinien być zastąpiony lub uzupełniony przez użytkownika w zależności od kontekstu, w którym występuje.
	Rysunki i diagramy wykonano zgodnie z notacją OMG Unified Modeling Language (UML) 2.0

1. Wprowadzenie

1.1 Terminologia

Tab. 1. Słownik terminów używanych w ramach systemu oraz jego dokumentacji.

Termin	Objaśnienie
PayByNet	Usługa polegająca m. in. na natychmiastowym przekazaniu informacji o przelewie z banku zleceniodawcy do beneficjenta.
KIR S.A. lub Izba	Krajowa Izba Rozliczeniowa S.A., operator usługi PayByNet.
Płatnik	Nabywca towarów, posiadający rachunek bankowy z uaktywnionym kanałem internetowego dostępu do rachunku.
Sprzedawca lub Sklep	Sprzedawca towarów, który podpisał z Izbą umowę o świadczenie usługi PayByNet. Specyfika sieci internetowej powoduje, że usługa jest skierowana głównie do podmiotów operujących w sieci (sklepy internetowe).
identyfikator Sprzedawcy	Unikalna w ramach systemu nazwa skrócona Sprzedawcy wskazana w Umowie na korzystanie z systemu PayByNet.
Bank	Bank udostępniający Płatnikowi usługę PayByNet na podstawie umowy łączącej Bank z Izbą.
identyfikator Banku	Unikalna w ramach systemu nazwa skrócona Banku wskazana w Umowie na korzystanie z systemu PayByNet.
płatność	Należność Płatnika na rzecz Sprzedawcy wynikająca z zawarcia przez Płatnika umowy kupna-sprzedaży ze Sprzedawcą.
informacja o płatności	Komplet informacji opisujących płatność, przetwarzany w ramach systemu PayByNet.
data ważności płatności	Dokładna data i godzina, do której należy dokonać płatności pod rygorem odstąpienia przez Sprzedawcę od umowy kupna-sprzedaży.
klient usługi	Sprzedawca lub Bank w ramach usługi PayByNet.
użytkownik usługi	Płatnik w ramach usługi PayByNet.
system PayByNet lub system	System informatyczny zaprojektowany i stworzony na potrzeby usługi PayByNet.
użytkownik systemu	Osoba lub system informatyczny uzyskujący dostęp do modułów systemu.
Funkcja haszująca/SHA-1	Algorytm używany do obliczania skrótu dla dowolnej wiadomości lub pliku danych dostarczonego na wejściu.

2. Opis systemu

2.1 Działanie systemu

Realizacja usługi PayByNet przebiega w rozproszonym środowisku sieciowym. W jej ramach następuje wymiana informacji między Sprzedawcą, Płatnikiem, Izbą oraz Bankiem.
Z punktu widzenia klientów systemu zewnętrznego efekty działania systemu PayByNet obejmują:

1. przekazywanie informacji o płatnościach Płatnika na rzecz Sprzedawców do Banku Płatnika,
2. prezentowanie Płatnikowi płatności na rzecz Sprzedawcy w ramach bankowości internetowej Banku Płatnika,
3. przekazywanie informacji o dokonanych przez Płatnika płatnościach na rzecz Sprzedawców do Izby,
4. prezentowanie Sprzedawcom informacji o płatnościach dokonanych na ich rzecz przez Płatników.

2.1.2 Przekazywanie informacji o płatnościach do Banku Płatnika

Przekazywanie informacji o płatnościach do Banku Płatnika obejmuje:

1. przekazanie przez Sprzedawcę, za pośrednictwem przeglądarki Płatnika, informacji o płatności na rzecz Sprzedawcy do Izby,
2. wybór przez Płatnika Banku w ramach witryny WWW Izby,
3. przekazanie przez Izbę, za pośrednictwem przeglądarki Płatnika, informacji o płatności na rzecz Sprzedawcy do Banku Płatnika,

przy czym:

1. Informacja o płatności przekazywana jest pomiędzy poszczególnymi uczestnikami wymiany informacji w postaci ciągu znaków umieszczonego w treści wywołania metody HTTP POST przesyłanej przez przeglądarkę Płatnika podczas kolejnych etapów przekazywania informacji.
2. Treść przekazywanej informacji o płatności jest zarówno przez Sprzedawcę, jak i Izbę, zabezpieczona funkcją haszującej SHA-1. W ramach systemu funkcja haszująca jest każdorazowo weryfikowany przez adresata po otrzymaniu informacji.
3. Konstrukcja systemu zakłada, że z każdą informacją o płatności skojarzona jest przez Sprzedawcę data ważności płatności, która weryfikowana jest podczas kolejnych etapów przekazywania informacji o płatności zarówno przez Izbę, jak i przez Bank Płatnika. Czas ważności transakcji określany jest przez Sprzedawcę indywidualnie dla każdej transakcji (lub dla wszystkich transakcji jest taki sam) i może zostać zawarty w przedziale czasowym od 15 minut do 7 dni.

2.1.3 Prezentowanie płatności w kanale internetowym Banku Płatnika

Prezentowanie płatności w kanale internetowym Banku Płatnika obejmuje:

1. wyświetlenie Płatnikowi płatności na rzecz Sprzedawcy w ramach bankowości internetowej Banku Płatnika, w sposób umożliwiający Płatnikowi jej zaakceptowanie lub odrzucenie, a jednocześnie minimalizujący możliwość pomyłki lub manipulacji w czasie dokonywania płatności;
2. uzyskanie potwierdzenia chęci dokonania bądź odrzucenia płatności w postaci przekazanej przez Izbę; przy czym zakłada się, iż działania te nie powinny wpływać na proces logowania Płatnika do kanału internetowego Banku ani na sposób i tryb akceptowania przez Płatnika płatności w ramach jego bankowości internetowej.

2.1.4 Przekazywanie informacji przez Bank o dokonanych płatnościach do Izby

Przekazywanie informacji o dokonanych płatnościach do Izby obejmuje aktualizację statusu płatności w bazie danych Izby na podstawie uzyskanego od Płatnika potwierdzenia chęci dokonania płatności o podanym wcześniej identyfikatorze płatności w relacji Izba-Bank, przy czym:

1. aktualizacja statusów płatności odbywa się za pomocą usługi sieciowej (WebService);
2. dostęp do dokumentu WSDL związanego z tą usługą odbywa się za pomocą protokołu HTTP;
3. w ramach usługi sieciowej Bank wywołuje metodę, która jako parametr przyjmuje dane podpisane za pomocą opracowanej przez Izbę biblioteki kryptograficznej, natomiast zwraca informacje o powodzeniu lub niepowodzeniu operacji aktualizując statusu płatności.

2.1.5 Prezentowanie Sprzedawcom informacji o płatnościach

Prezentowanie Sprzedawcom informacji o płatnościach obejmuje:

1. Powiadamianie Sprzedawców o zmianie statusu dotyczących ich płatności poprzez pocztę elektroniczną. W tym wariancie Sprzedawca po otrzymaniu wiadomości pocztowej o zmianie statusu płatności łączy się, przy wykorzystaniu informacji znajdujących się w wiadomości pocztowej, z witryną internetową Izby w celu zweryfikowania statusu transakcji.(wariant 1)
2. Powiadamianie Sprzedawców o zmianie statusu dotyczących ich płatności za pomocą usługi sieciowej Web Service. (wariant 2 lub wariant 3)

2.2 Specyfikacja

2.2.1 Bezpieczeństwo wymiany informacji miedzy stronami – użytkownikami i klientami usługi PayByNet

Bezpieczeństwo wymiany informacji między stronami – użytkownikami i klientami usługi PayByNet jest zapewnione poprzez zastosowanie w ramach systemu PayByNet w Izbie następujących mechanizmów:

1. W relacji Izba-Bank oraz Bank-Izba uwierzytelnienie oraz poufność informacji o płatnościach zapewniona jest poprzez:
    - przez Izbę, przy użyciu klucza prywatnego Izby (w relacji Izba-Bank),
    - przez Bank, przy użyciu klucza prywatnego Banku (w relacji Bank-Izba),
    - wymiana informacji prowadzona jest w dedykowanej sieci bankowej
2. w relacji Izba-Sprzedawca, Sprzedawca-Izba:
    - stosując algorytm SHA-1
    - protokołu SSL,
    - przez Sprzedawcę, przy użyciu klucza prywatnego Sprzedawcy (w relacji Sprzedawca-Izba),

Podpisywanie i weryfikowanie podpisów elektronicznych wykonywane jest przy wykorzystaniu dedykowanej biblioteki kryptograficznej opracowanej przez Izbę i udostępnionej klientom usługi PayByNet.

2.2.2 Zastosowanie protokołu SSL

W ramach systemu w komunikacji między użytkownikami i modułami systemu PayByNet stosowane są połączenia SSL szyfrowane kluczem o długości 128 bitów.

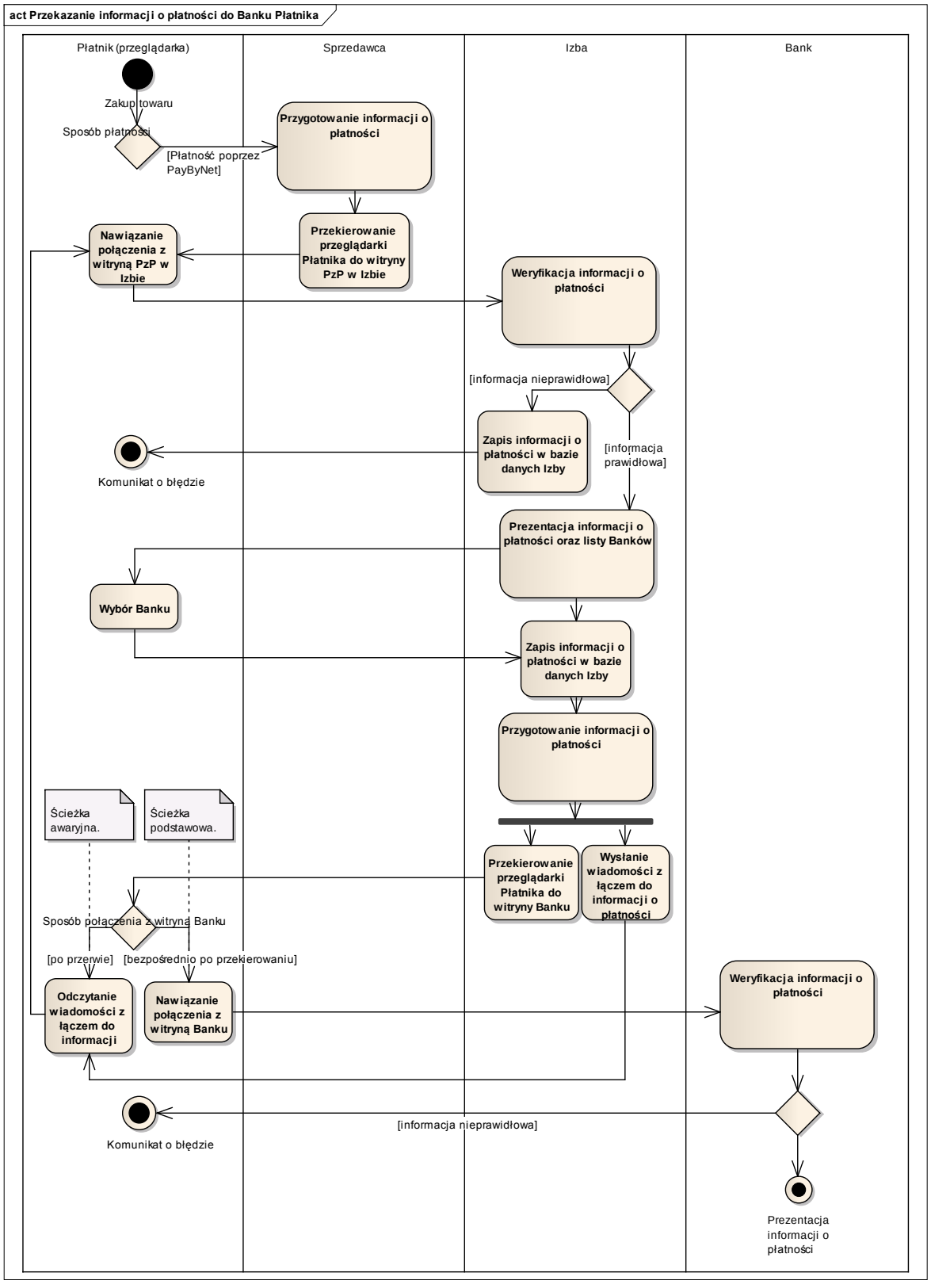
2.2.3 Interfejs użytkownika

Interfejs obsługi i zarządzania systemem PayByNet został zrealizowany w postaci szeregu stron WWW dostępnych dla autoryzowanych użytkowników systemu. Dostęp do interfejsu systemu możliwy jest wyłącznie poprzez wywołanie w przeglądarce internetowej adresu https://pbn.paybynet.com.pl/PayByNetT/login.do dla środowiska testowego PayByNet lub https://pbn.paybynet.com.pl/PayByNet/login.do dla środowiska produkcyjnego PayByNet oraz poprawną autoryzację w oknie logowania.
Użytkownikom uzyskującym dostęp do modułu systemu autoryzuję się w ramach systemu PayByNet za pomocą *nazwy użytkownika i hasła.*

2.3 Specyfikacja funkcjonalna

2.3.1 Przekazywanie informacji o płatnościach do Banku Płatnika

Rys. 1. Diagram przedstawiający przekazywanie informacji o płatnościach.



2.4 Przygotowanie informacji o płatności przez Sprzedawcę

System PayByNet wymaga aby zbiór informacji przesyłanych do systemu był zabezpieczony przy użyciu funkcji skrótu SHA-1

2.4.1 Przygotowanie informacji o płatności przez Sprzedawcę stosującego metodę funkcji skrótu SHA-1

1. Po wybraniu przez Płatnika jako metody dokonania płatności usługi PayByNet, serwer sklepu Sprzedawcy przygotowuje do wysłania do Izby informację o płatności:

Tab. 2 Zawartość informacji o płatności kierowanej przez Sprzedawcę do Izby.

Pole	Opis	Format	Przykładowa wartość
id_client	Identyfikator (NIP) Sprzedawcy wskazany w Umowie na korzystanie z systemu PayByNet.	numer NIP z opcjonalnym dodatkowym, jednoznakowym wyróżnikiem, długość minimalna 10 znaków, długość maksymalna 11 znaków, pole obowiązkowe, wartość musi być unikalna w ramach systemu PayByNet	1234567890 lub 12345678901
id_trans	Jednoznaczny identyfikator płatności w relacji Sprzedawca-Izba.	ciąg cyfr i liter długość 10 znaków alfanumerycznych, pole obowiązkowe	32121ABC23 lub 1234567890 lub ABCDEFGHIJ
date_valid	Data i godzina ważności płatności.	ciąg cyfr w formacie dd-mm-yyyy hh:MM:ss, długość 19 znaków, pole obowiązkowe	27-04-2005 12:33:51
amount	Kwota płatności.	wartość w formacie NNNNNNNN,nn gdzie: NN – części całe, , - separator części całych i dziesiętnych (przecinek), nn – części dziesiętne, długość maksymalna 11 znaków, pole obowiązkowe	49,90
currency	Waluta płatności.	identyfikator waluty; obecnie parametr ten może przyjmować wyłącznie wartość „PLN” oznaczającą złote polskie, długość 3 znaki, pole obowiązkowe	PLN
email	Adres poczty elektronicznej Płatnika.	adres email, długość maksymalna 100 znaków, pole opcjonalne	imie.nazwisko@wp.pl
account	Numer rachunku bankowego Sprzedawcy.	numer NRB Sprzedawcy, długość 26 znaków,	12231231230000000032331127

Pole	Opis	Format	Przykładowa wartość
		pole obowiązkowe	
accname	Nazwa rachunku bankowego Sprzedawcy.	ciąg znaków alfanumerycznych. Poszczególne składniki nazwy rozdzielone są znakami kodowymi (opisującymi), umieszczonymi za częścią opisywaną: ^NM^ - nazwa ^ZP^ - kod ^CI^ - miasto ^ST^ - ulica ^CT^ - kraj długość maksymalna 140 znaków, kolejność poszczególnych składników obowiązkowa pole obowiązkowe	ShopOnLine e-sklep^NM^02-001^ZP^Warszawa^CI^ul.Klonowa 33^ST^Polska^CT^
backpage	Adres URL, pod który ma zostać przekierowana przeglądarka Płatnika po prawidłowym dokonaniu płatności.	adres URL, długość maksymalna 255 znaków, pole obowiązkowe	http://shop.online.pl/ShopOnLine/find.do?end=1
backpagereject	Adres URL, pod który ma zostać przekierowana przeglądarka Płatnika po odrzuceniu płatności przez Płatnika lub Bank oraz w przypadku powrotu do Sklepu przed wybraniem Banku.	adres URL, długość maksymalna 255 znaków, pole nieobowiązkowe	http://shop.online/ShopOnline/find.do?end=2
Hash	Skrót z transakcji z użyciem SHA-1	Ciąg znaków skrótu w zapisie szesnastkowym - stała długość 40 znaków. Pole obowiązkowe	<hash>fc4d111df1f8868e66e6fe8393b568434ac4d94</hash>
automat	Pole określające sposób zachowania systemu – obsługa bez przekierowania	Wymagana wartość true	<automat>true</automat>

przy czym:

a) w informacji o płatności powinny znaleźć się wszystkie pola, które zostały oznaczone w kolumnie „Format” jako obowiązkowe,
b) wszystkie pola powinny zostać scalone w ciąg o postaci:

<nazwa_pola_1>wartość_pola</nazwa_pola_1><nazwa_pola_2>wartość_pola_2</nazwa_pola_2>...<nazwa_pola_n>wartość_pola_n</nazwa_pola_n>

c) po poprawnym zebraniu informacji konieczne jest zakodowanie informacji w formacie base64

Przyjmowana transakcja zakodowana w base64 w polu formularza o nazwie **SHA-1** będzie zawierać dodatkowe pole zawierające skrót SHA-1 z całej transakcji (*<hash>*).

Budowanie skrótu będzie odbywać się przez dodanie do transakcji nowego znacznika *<password>xxxx</password>* i wygenerowanie skrótu *SHA-1* . Po tej operacji znacznik *<password>* zostaje zastąpiony znacznikiem *<hash>* W ten sposób zakodowana transakcja (base64) jest przekazana do systemu.

Przykład poprawnie zbudowanej płatności przed użyciem algorytmu SHA-1:

Krok 1: przygotowanie danych zgodnie z tabelką

<id_client>5267367878</id_client><id_trans>1276246666</id_trans><date_valid>11-06-2010 11:57:46</date_valid><amount>1,99</amount><currency>PLN</currency><email> </email><account>21114011409876543210123456</account><accname>ShopOnline1 e-sklep^NM^02-001^ZP^Warszawa^CI^ul.Klonowa33^ST^Polska^CT^</accname> <backpage>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=1</backpage><backpagereject>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject> <password>qwerty123456</password>

Krok 2: Szyfrowanie
Kolorem niebieskim zaznaczone są dane które muszą zostać zaszyfrowane i wstawione w pole <hash></hash>:

<id_client>5267367878</id_client><id_trans>1276246666</id_trans><date_valid>11-06-2010 11:57:46</date_valid><amount>1,99</amount><currency>PLN</currency><email> </email><account>21114011409876543210123456</account><accname>ShopOnline1 e-sklep^NM^02-001^ZP^Warszawa^CI^ul.Klonowa33^ST^Polska^CT^</accname> <backpage>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=1</backpage><backpagereject>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject> <hash><id_client>5267367878</id_client><id_trans>1276246666</id_trans><date_valid>11-06-2010 11:57:46</date_valid><amount>1,99</amount><currency>PLN</currency><email> </email><account>21114011409876543210123456</account><accname>ShopOnline1 e-sklep^NM^02-001^ZP^Warszawa^CI^ul.Klonowa33^ST^Polska^CT^</accname> <backpage>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=1</backpage><backpagereject>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject> <password>qwerty123456</password></hash>

Po wykonaniu powyższej operacji z użyciem algorytmu SHA-1 otrzymujemy wartość:

<id_client>5267367878</id_client><id_trans>1276246666</id_trans><date_valid>11-06-2010 11:57:46</date_valid><amount>1,99</amount><currency>PLN</currency><email> </email><account>21114011409876543210123456</account><accname>ShopOnline1 e-sklep^NM^02-001^ZP^Warszawa^CI^ul.Klonowa33^ST^Polska^CT^</accname> <backpage>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=1</backpage><backpagereject>http://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject> <hash>694be6ddcafdd79f2f1e1c2d261af2167cd9a6a4</hash>

Krok 3: Kodowanie algorytmem base64
Ostatnim krokiem jest użycie algorytmu base64 i zakodowanie informacji :

hashtrans=PGlkX2NsaWVudD41MjY3MzY3ODc4PC9pZF9jbGllbnQ+PGlkX3RyYW5zPjEyNzYyNDY2NjY8L2lkX3RyYW5zPjxkYXRlX3ZhbGlkPjExLTA2LTIwMTAgMTE6NTc6NDY8L2RhdGVfdmFsaWQ+PGFtb3VudD4

xLDk5PC9hbW91bnQ+PGN1cnJlbmN5PlBMTjwvY3VycmVuY3k+PGVtYWlsPgo8L2VtYWlsPjxhY2NvdW50PjIxMTE0MDExNDA5ODc2NTQzMjEwMTIzNDU2PC9hY2NvdW50PjxhY2NuYW1lPlNob3BPbmxpbmUxIAplLXNrbGVwXk5NXjAyLTAwMV5aUF5XYXJzemF3YV5DSV51bC5LbG9ub3dhMzNeU1ReUG9sc2thXkNUXjwvYWNjbmFtZT4KPGJhY2twYWdlPmh0dHA6Ly9wYnluYzMucGJuLmtpci5jb20ucGwvU2hvcE9ubGluZUQvZmluZC5kbz9lbmQ9MTwvYmFja3BhZ2U+PGJhY2twYWdlcmVqZWN0Pmh0dHA6Ly9wYnluYzMucGJuLmtpci5jb20ucGwvU2hvcE9ubGluZUQvZmluZC5kbz9lbmQ9MjwvYmFja3BhZ2VyZWplY3Q+CjxoYXNoPjY5NGJlNmRkY2FmZGQ3OWYyZjFlMWMyZDI2MWFmMjE2N2NkOWE2YTQ8L2hhc2g+Cg==

Tak przygotowaną transakcję można przesłać do systemu PayByNet.

Hasło z którego zostanie zbudowana funkcja skrótu nie powinno być krótsze niż 8 znaków oraz nie dłuższe niż 40 znaków alfanumerycznych. Przekazywanie hasła będzie odbywało się w następujący sposób:

- Upoważniony przedstawiciel Sklepu przygotowuje i zapisuje hasło w pliku txt
- Plik txt zawierający hasło należy wysłać na adres paybynet@paybynet.pl

Jeżeli wystąpi podejrzenie, że hasło do generowania funkcji skrótu mgło zostać poznane przez osoby niepowołane, istnieje możliwość zmiany hasła wykorzystując metodę przedstawioną powyżej.

2.4.1.2 Przekierowanie przeglądarki Płatnika do witryny PayByNet

Przekierowanie przeglądarki Płatnika do witryny PayByNet w Izbie obejmuje:
umieszczenie zakodowanej informacji o płatności w treści wywołania metody HTTP POST odwołującego się do URL witryny PayByNet w Izbie, w polu o nazwie hashtrans, np:

hashtrans=aWRfY2xpZW50PVNob3BPbkxpbmU7aWRfdHJhbnM9MTExNDYwNjM2NDtkYXRlX3ZhbGlkPTI3LTA0LTIwMDU7YW1vdW50PTQ5LDkwO2FjY291bnQ9MTIgMjMxMiAzMTIzIDAwMDAgMDAwMCAzMjMzIDExMjc7YmFja3BhZ2U9aHR0cDovL2xvY2FsaG9zdDo4MDgwL1Nob3BPbkxpbmUvZmluZC5kbz9lbmQ9MQ0KO3NpZz1Xd2hrcURNSXA2dnBsMUtocXEvRGk3NDJ0eDRGU1o4NlE2a0wvaEFhdU92MkI0NGF3QnRWUERsUVBXTUNQYnFBK1BLN1NJY2VqSVRLZENNcXFOaGY3c3R3blM2MW12Yk4yQThuS25qZnp6N2Q5bTZlL2V5RmtaT3h3OUE4eDNaMDY1RkVUSG9SZjAralgxeGhXNEpMTDQ0eW42ZktvTGhqUWRldTlraTc3T2s9[...]

Przekierowanie przeglądarki płatnika pod adres witryny PayByNet w Izbie:
dla środowiska testowego PayByNet - https://pbn.paybynet.com.pl/PayByNetT/trans.do
dla środowiska produkcyjnego PayByNet - https://pbn.paybynet.com.pl/PayByNet/trans.do

2.4.1.3 Zapis transakcji w systemie bez przekierowania

Zastosowanie w przekazanej transakcji parametru <automat> ustawionego na **true** powoduje standardowe zapisanie transakcji w systemie jednak bez przekierowania na witrynę PayByNet. Wynikiem wywołania takiej transakcji jest strona html :

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pl" lang="pl"
dir="ltr">
<head>
<meta http-equiv="Content-type" content="text/html; charset=UTF-8" />
<title>PayByNet</title>
```

```
</head>
<body>
 <form action="">
   <input name="status" type="text" value="<wartość_statusu>">
   <input name="info" type="text" value="<wartość_opisowa>">
   <input name="link" type="text" value="<link do transakcji>">
 </form>
</body>
</html>
```

Poszczególne wartości parametrów oznaczają :

- Status – wartość 0 – transakcja przyjęta i zapisana w systemie ; wartość 1 – błąd zapisu transakcji,
- Info – wartość opisowa ewentualnego błędu w przyjęciu transakcji (pole status = 1)
- Link – link url do zapisanej transakcji w systemie (tylko dla status = 0)

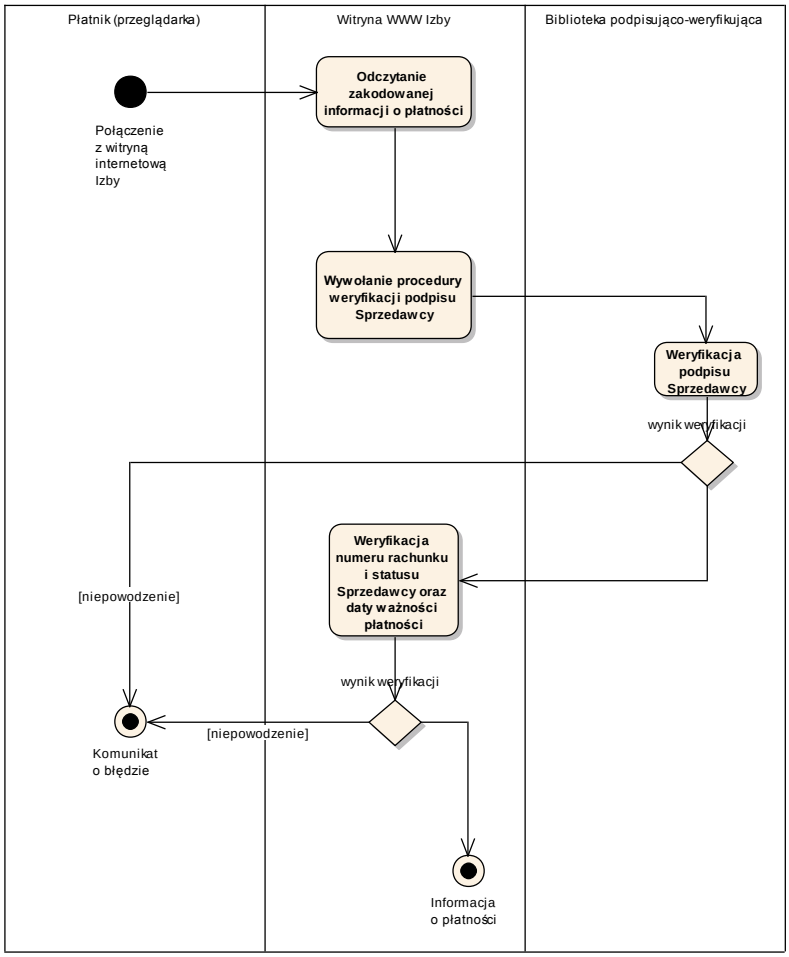
2.4.1.4 Weryfikacja informacji o płatności (Izba)

Weryfikacja informacji o płatności obejmuje:

1. odczytanie zakodowanej informacji o płatności. Oprogramowanie serwera WWW Izby odczytuje zawartość pola **hashtrans** z treści wywołania metody HTTP POST,
2. rozkodowanie informacji, porównanie funkcji skrótu. System rozkodowuje transakcję, znacznik *<hash>* zstępowany jest znacznikiem *<password>* z wartością pobraną z bazy danych systemu. System generuje skrót SHA-1 i porównuje go z przekazanym przez Sklep.
3. weryfikacja daty ważności płatności. System porównuje bieżącą datę z datą ważności płatności i jeżeli bieżąca data ma wartość większą niż data ważności płatności, wyświetlić stosowny komunikat na o błędzie,
4. weryfikacja poprawności logicznej i formalnej numeru rachunku bankowego Sprzedawcy. System kontroluje zgodność rachunku bankowego ze standardem NRB oraz dodatkowo weryfikuje jego poprawność z listą zdefiniowanych rachunków danego Sprzedawcy w bazie danych Systemu.

2.4.1.5 Weryfikacja informacji o płatności (Izba)

Rys. 2. Weryfikacja informacji o płatności (Izba).



Weryfikacja informacji o płatności obejmuje:

1. odczytanie zakodowanej informacji o płatności. Oprogramowanie serwera WWW Izby odczytuje zawartość pola **hashtrans** z treści wywołania metody HTTP POST,
2. wywołanie procedury weryfikacji podpisu Sprzedawcy. Oprogramowanie wywołuje procedurę, w wyniku której podpis elektroniczny Sprzedawcy pod informacją o płatności zostaje zweryfikowany.
3. weryfikacja daty ważności płatności. System porównuje bieżącą datę z datą ważności płatności i jeżeli bieżąca data ma wartość większą niż data ważności płatności, wyświetlić stosowny komunikat na o błędzie,
4. weryfikacja poprawności logicznej i formalnej numeru rachunku bankowego Sprzedawcy. System kontroluje zgodność rachunku bankowego ze standardem NRB oraz dodatkowo weryfikuje jego poprawność z listą zdefiniowanych rachunków danego Sprzedawcy w bazie danych Systemu.

2.5 Zapis informacji o płatności w bazie danych Izby

Zapis informacji o płatności w bazie danych Izby następuje:

a) gdy wynik weryfikacji płatności jest negatywny:
   - gdy informacja o płatności jest uszkodzona, w wyniku czego nie jest możliwe jej odszyfrowanie,
   - gdy weryfikacja podpisu elektronicznego lub funkcji haszującej Sprzedawcy kończy się niepowodzeniem,
   - gdy upłynęła już data ważności płatności,
   - gdy Sprzedawca ma status „nieaktywny”,
   - gdy Sprzedawca jest poza zakresem dat aktywności,
   - gdy rachunek nie jest zgodny z formatem NRB,

b) gdy wynik weryfikacji płatności jest pozytywny:
   - gdy Płatnik dokona wyboru Banku (informacja o płatności zostaje zapisana w bazie danych Izby i system kontynuuje przekazywanie płatności do wybranego przez Płatnika Banku),
   - w przypadku, gdy Płatnik nie dokona wyboru Banku (informacja o płatności zostaje zapisana w bazie danych Izby, lecz – wobec braku wskazania Banku przez Płatnika - system nie kontynuuje dalej przekazywania płatności).

2.6 Przygotowanie informacji o płatności i przesłanie do banku (Izba)

Po zapisaniu informacji o płatności w bazie danych Izby, serwer witryny WWW Izby przygotowuje do wysłania do Banku informację o płatności. Następuje wywołanie, za pośrednictwem biblioteki kryptograficznej, metody podpisującej i kodującej informację o płatności. Wynikiem działania procedury jest zakodowana w standardzie Base64 struktura PKCS#7 zawierająca:

- dane wejściowe,
- podpis,
- certyfikat z kluczem publicznym nadawcy (KIR).

2.7 Przekierowanie przeglądarki Płatnika do witryny Banku Płatnika

Przekierowanie przeglądarki Płatnika do witryny Banku Płatnika obejmuje:

1. umieszczenie zakodowanej informacji o płatności w treści wywołania metody HTTP POST odwołującego się do URL witryny Banku Płatnika.
2. przekierowanie przeglądarki płatnika pod adres witryny Banku Płatnika, np.: https://bank.com.pl

2.8 Przekazywanie informacji o statusie płatności dla Sprzedawcy

Tab. 3 Prezentowanie przez Izbę Sprzedawcom informacji o dokonanych przez Płatników płatnościach.

Czynność	Opis
Izba lub Bank	aktualizuje status płatności w bazie danych Izby
Izba	odczytuje dane Sprzedawcy, któremu przyporządkowana jest płatność
wariant 1 – email	
Izba	informuje Sprzedawcę statusie płatności przy użyciu wiadomości poczty elektronicznej (SMTP) z zawartym łączem do informacji o płatności w bazie danych Izby
Sprzedawca	łączy się przy użyciu protokołu HTTPS ze wskazanym przez Izbę serwerem WWW
Izba	wyświetla formularz logowania do systemu PayByNet
Sprzedawca	uwierzytelnia się przy użyciu identyfikatora użytkownika i hasła
Izba	prezentuje informację o płatności
	zapisuje informacje o odczytaniu statusu płatności przez Płatnika w bazie płatności
wariant 2 – WebService (rekomendowany w przypadku konieczności dokonywania dużej ilości powiadomień)	
Sprzedawca	wywołuje po stronie Izby WebService z odpowiednimi parametrami w celu odczytania statusu płatności.
Przykład wywoływania metody	getStatusByPaymentID(String paymentID,String clientID, Double amount) getStatusByPaymentID(String paymentID,String clientID) paymentID - identyfikator płatności klienta clientID - identyfikator klienta amount - kwota
wariant 3 – WebService (rekomendowany w przypadku konieczności dokonywania dużej ilości powiadomień) **WAŻNE: Wybranie tej metody powiadomienia jest możliwe po wcześniejszym ustaleniu z pracownikiem KIR koordynującym wdrożenie**	
Izba	wywołuje po stronie sprzedawcy WebService z odpowiednimi parametrami w celu aktualizacji statusu transakcji

Szczegółowy opis usługi sieciowej tworzonej po stronie klienta systemu PayByNet, służącej dostarczaniu informacji na temat statusów transakcji zarejestrowanych w systemie - Wariant 3

Nazwa usługi: PayByNetGatewayService.
Nazwa metody: transactionStatusChanged
Parametr metody: String, postać:
<transaction><id_trans>paymentID</id_trans><status>transStatus</status></transaction>

paymentID: identyfikator płatności (id transakcji nadane przez system sklepu).
transStatus: status transakcji.

Bramka PayByNetGatewayService powinna obsługiwać deskryptor WSDL (opisujący punkt dostępowy WebService) w specyfikacji:

WSDL 1.1 - http://www.w3.org/TR/2001/NOTE-wsdl-20010315

Komunikaty XML są obsługiwane zgodnie ze specyfikacją:

SOAP 1.1 - http://www.w3.org/TR/2000/NOTE-SOAP-20000508/ w dialekcie:
soap:binding style="document"
transport= http://schemas.xmlsoap.org/soap/http/

Przykład pliku WSDL:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions name="PayByNetGatewayService" targetNamespace="http://adres_serwera/"
xmlns:ns1="http://cxf.apache.org/bindings/xformat" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://adres_serwera/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <wsdl:types>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="unqualified"
targetNamespace="http://adres_serwera/" xmlns:tns="http://adres_serwera/"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="transactionStatusChanged" type="tns:transactionStatusChanged"/>
<xs:element name="transactionStatusChangedResponse" type="tns:transactionStatusChangedResponse"/>
<xs:complexType name="transactionStatusChanged">
<xs:sequence>
<xs:element minOccurs="0" name="arg0" type="xs:string"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="transactionStatusChangedResponse">
<xs:sequence/>
</xs:complexType>
<xs:element name="GatewayProcessingException" type="tns:GatewayProcessingException"/>
<xs:complexType name="GatewayProcessingException">
<xs:sequence/>
</xs:complexType>
</xs:schema>
  </wsdl:types>
  <wsdl:message name="GatewayProcessingException">
    <wsdl:part element="tns:GatewayProcessingException" name="GatewayProcessingException">
```

```
  </wsdl:part>
 </wsdl:message>
 <wsdl:message name="transactionStatusChangedResponse">
  <wsdl:part element="tns:transactionStatusChangedResponse" name="parameters">
  </wsdl:part>
 </wsdl:message>
 <wsdl:message name="transactionStatusChanged">
  <wsdl:part element="tns:transactionStatusChanged" name="parameters">
  </wsdl:part>
 </wsdl:message>
 <wsdl:portType name="PayByNetGateway">
  <wsdl:operation name="transactionStatusChanged">
   <wsdl:input message="tns:transactionStatusChanged" name="transactionStatusChanged">
  </wsdl:input>
   <wsdl:output message="tns:transactionStatusChangedResponse"
name="transactionStatusChangedResponse">
  </wsdl:output>
   <wsdl:fault message="tns:GatewayProcessingException" name="GatewayProcessingException">
  </wsdl:fault>
  </wsdl:operation>
 </wsdl:portType>
 <wsdl:binding name="PayByNetGatewayServiceSoapBinding" type="tns:PayByNetGateway">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="transactionStatusChanged">
   <soap:operation soapAction="" style="document"/>
   <wsdl:input name="transactionStatusChanged">
    <soap:body use="literal"/>
   </wsdl:input>
   <wsdl:output name="transactionStatusChangedResponse">
    <soap:body use="literal"/>
   </wsdl:output>
   <wsdl:fault name="GatewayProcessingException">
    <soap:fault name="GatewayProcessingException" use="literal"/>
   </wsdl:fault>
  </wsdl:operation>
 </wsdl:binding>
 <wsdl:service name="PayByNetGatewayService">
  <wsdl:port binding="tns:PayByNetGatewayServiceSoapBinding" name="PayByNetGatewayPort">
   <soap:address location="http://adres_uslugi"/>
  </wsdl:port>
 </wsdl:service>
</wsdl:definitions>
```

2.9 Statusy płatności w systemie PayByNet