Specyfikacja interfejsów dla Sklepów

KIR Paybynet

Spis treści

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

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.

2.2 Przekazywanie informacji o płatnościach do Banku

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.

2.3 Prezentowanie płatności w kanale internetowym Banku Płatnika

Prezentowanie płatności w kanale internetowym Banku Płatnika obejmuje:
wyświetlenie Płatnikowi automatycznie uzupełnionej płatności na rzecz Sprzedawcy w ramach bankowości internetowej Banku Płatnika, w sposób umożliwiający Płatnikowi jej zaakceptowanie lub odrzucenie. Płatnik nie ma możliwości dokonania żadnych zmian w treści przelewu.

3. Specyfikacja

3.1 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.

3.2 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,	27-04-2005 12:33:51

Pole	Opis	Format	Przykładowa wartość
		pole obowiązkowe; czas ważności można regulować w zakresie od 15 minut do 7 dni	
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; długość 3 znaki, pole obowiązkowe	PLN, GBP, EUR, USD
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, pole obowiązkowe	12231231230000000032331127
accname	Nazwa 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 obowiązkowe	http://shop.online/ShopOnline/find.do?end=2

Pole	Opis	Format	Przykładowa wartość
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 Pole opcjonalne Opis wykorzystania tego parametru znajduje się w punkcie 3.6 dokumentacji.	<automat>true</automat>
description	Dodatkowy opis transakcji przekazany do pola „Tytułem”	Pole opcjonalne. Maksymalna długość 30 znaków. Dozwolone znaki: . , / \ :-	<description>dodatkowy opis transakcji </description>

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><description>dodatkowy opis transakcji</description><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>h
ttp://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject><description>dodatkowy
opis transakcji</description><
<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>h
ttp://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject><description>dodatkowy
opis transakcji</description><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>h
ttp://pbync3.pbn.kir.com.pl/ShopOnlineD/find.do?end=2</backpagereject><description>dodatkowy
opis transakcji</description><hash>694be6ddcafdd79f2f1e1c2d261af2167cd9a6a4</hash>

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

hashtrans=PGlkX2NsaWVudD41MjY3MzY3ODc4PC9pZF9jbGllbnQ+PGlkX3RyYW5zPjEyNzYyNDY2NjY8L
2lkX3RyYW5zPjxkYXRlX3ZhbGlkPjExLTA2LTIwMTAgMTE6NTc6NDY8L2RhdGVfdmFsaWQ+PGFtb3VudD4
xLDk5PC9hbW91bnQ+PGN1cnJlbmN5PlBMTjwvY3VycmVuY3k+PGVtYWlsPgo8L2VtYWlsPjxhY2NvdW50
PjIxMTE0MDExNDA5ODc2NTQzMjEwMTIzNDU2PC9hY2NvdW50PjxhY2NuYW1lPlNob3BPbmxpbmUxIA
plLXNrbGVwXk5NXjAyLTAwMV5aUF5XYXJzemF3YV5DSV51bC5LbG9ub3dhMzNeU1ReUG9sc2thXkNUXj
wvYWNjbmFtZT4KPGJhY2twYWdlPmh0dHA6Ly9wYnluYzMucGJuLmtpci5jb20ucGwvU2hvcE9ubGluZUQ
vZmluZC5kbz9lbmQ9MTwvYmFja3BhZ2U+PGJhY2twYWdlcmVqZWN0Pmh0dHA6Ly9wYnluYzMucGJuL
mtpci5jb20ucGwvU2hvcE9ubGluZUQvZmluZC5kbz9lbmQ9MjwvYmFja3BhZ2VyZWplY3Q+CjxoYXNoPjY
5NGJlNmRkY2FmZGQ3OWYyZjFlMWMyZDI2MWFmMjE2N2NkOWE2YTQ8L2hhc2g+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.

3.3 Przekierowanie Płatnika do systemu 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

3.4 Obsługa rachunków wirtualnych (tzw. masscollect)

W systemie Paybynet możliwa jest również obsługa rachunków wirtualnych. W tym przypadku numer rachunku bankowego musi być przesyłany do systemu Paybynet w odpowiedni sposób. Poniżej prezentacja przykładowego numeru rachunku bankowego z nałożoną maską:

123456789011********

3.5 Przekierowanie Płatnika ze strony sklepu do banku – wybór banku na stronie sklepu

W systemie Paybynet istnieje możliwość, aby wybór banku następował na stronie sklepu (z pominięciem wyboru banku na witrynie Paybynet). Działanie polega na podpięciu przez sklep dedykowanego adresu URL do odpowiedniej ikony banku. Klient klikając w ikonę banku będzie automatycznie przeniesiony do bankowości elektronicznej. Pozostałe funkcje systemu pozostają bez zmian.
Wyjątek stanowi przekierowanie dla Banków Spółdzielczych. W związku z dużą ilością Banków Spółdzielczych przekierowanie w tym przypadku odbywa się przez witrynę Paybynet gdzie po pomocą mapy z podziałem administracyjnym Płatnik wybiera swój bank.
Przykładowy link przekierowania do banków wygląda następująco:

https://pbn.paybynet.com.pl/PaybynetT/trans.do?idbank=15401157

Dedykowane l inki do banków działających w systemie produkcyjnym będą przesyłane do zainteresowanego sklepu indywidualnie mailem.

3.6 Zapis transakcji w systemie bez przekierowania do banku

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)

3.7 Weryfikacja informacji o płatności (Izba)

Weryfikacja informacji o płatności obejmuje:

1. odczytanie zakodowanej informacji o płatności. System 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.

4. Przesyłanie informacji o statusie transakcji – opis metod

Wariant 1 – przesyłanie statusów na wskazany przez sprzedawcę adres email.
Wariant 2 – status przesyłany jest za pośrednictwem WebService. Sprzedawca wywołuje po stronie Izby WebService z odpowiednimi parametrami w celu odczytania statusu płatności
Przykład wywoływania metody dla tego wariantu:

getStatusByPaymentID(String paymentID,String clientID, Double amount)
getStatusByPaymentID(String paymentID,String clientID)

paymentID - identyfikator płatności klienta
clientID - identyfikator klienta
amount - kwota

Wariant 3 – przekazanie statusu do sklepu metodą POST – wariant rekomendowany.

WAŻNE: W celu uruchomienia koniecznej jest przekazanie do KIR adresu URL na który mają być wysyłane statusy transakcji

Rozwiązanie pozwala na powiadamianie sklepu/klienta o zmianie statusu transakcji z wykorzystaniem metody POST na określony przez URL. Wywołanie po stronie systemu Paybynet ma postać :

(Przykład formatu danych)
newStatus=%newStatus%&transAmount=%transAmount%&paymentId=%paymentId%&hash=%hash%

gdzie odpowiednio parametry:
newStatus – status transakcji.
transAmount – kwota transakcji.
paymentId – identyfikator transakcji przekazane ze sklepu.
hash – skrót SHA1 z połączenia : newStatus + transAmount + paymentId + password

gdzie password to hasło ustalone ze sklepem w celu wymiany informacji.
W wyniku wywołania system sklepu/klienta zwraca ciąg znaków „OK", każda inna odpowiedz oznacza niedostarczenie powiadomienia.

5. Statusy płatności w systemie Paybynet

W systemie Paybynet funkcjonują poniższe statusy transakcji:
2203 oraz 2303 – transakcja zatwierdzona – klient w bankowości elektronicznej zatwierdził przygotowana płatność. Sprzedawca otrzyma wpłatę na swoje konto.
2202 oraz 2302 – transakcja odrzucona – klient odrzucił w bankowości przygotowany przelew lub nie posiadał na swoim koncie pieniędzy w ilości wystarczającej na opłacenie transakcji.
2201 oraz 2301 – transakcja przeterminowana – klient nie wykonał transakcji, dodatkowo upłynął czas ważności transakcji określony przez sprzedawcę.

Dodatkowo w systemie występują statusy pośrednie (przy Wariancie 2), są to:
2101 – oczekująca na wybór banku
2102 – skierowana do banku