Specyfikacja integracji Serwisu Partnera z Systemem Płatności Online Blue Media w zakresie obsługi transakcji i rozliczeń

Projekt	**System Płatności Online Blue Media**
Autorzy	Michał Frozyna, Łukasz Łobocki, Krystian Wesołowski
Tytuł	Specyfikacja integracji Serwisu Partnera z Systemem Płatności Online Blue Media w zakresie obsługi transakcji i rozliczeń.
Rodzaj	Dokumentacja techniczna
Opis dokumentu	Dokument przedstawia specyfikację integracji Serwisu Partnera z Systemem Płatności Online Blue Media.
Wersja	2.22.1

Definicje

Poniższe definicje stanowią ogół pojęć stosowanych w niniejszym dokumencie oraz ewentualnych dokumentach powiązanych.

Aplikacja – Aplikacja Mobilna Partnera, komunikująca się z SDK Systemu Płatności Online BM w celu rejestrowania Transakcji.
BM – Blue Media Spółka Akcyjna z siedzibą w Sopocie przy ulicy Powstańców Warszawy 6, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000320590, NIP 585-13-51-185, Regon 191781561, o kapitale zakładowym w wysokości 2 000 000 PLN (w całości opłaconym), nadzorowana przez Komisję Nadzoru Finansowego i wpisana do rejestru krajowych instytucji płatniczych pod numerem IP17/2013, właściciel Systemu.
ClientHash - parametr w komunikatach; pozwala w sposób zanonimizowany przypisać Instrument płatniczy (np. Kartę) do Klienta. Na jego podstawie Partner może wywoływać kolejne obciążenia w modelu płatności automatycznych.
Dzień Roboczy – dzień tygodnia od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
Dodatek – dokument powiązany zawierający dodatkowe informacje i schematy dotyczące podstawowych usług oraz zaawansowane opcje Systemu (m.in. transakcje w tle, parametry dodatkowe, operacje na transakcjach, weryfikacje tożsamości płatnika, płatności automatyczne - cykliczne i jednym kliknięciem).
iFrame – jest to metoda przyjmowania płatności Kartą za produkty/usługi oferowane przez Partnera, w której dane Karty wprowadzane są przez Klienta w dostarczonym przez BM dokumencie HTML, osadzonym bezpośrednio w Serwisie. Aby wywołać formatkę kartową, Partner powinien zaimplementować specjalny kod JavaScript (skryptowy język programowania) wykorzystujący dedykowaną dla tego rozwiązania bibliotekę BM.
Instrument Płatniczy (lub zamiennie Kanał Płatności) – uzgodniony przez Klienta i jego dostawcę zbiór procedur lub zindywidualizowane urządzenie, wykorzystywane przez Klienta do złożenia zlecenia płatniczego np. Karta, PBL.
Instrument Płatniczy BM (Zwrot) – uzgodniony przez Partnera i BM zbiór procedur lub zindywidualizowane urządzenie, wykorzystywane przez Partnera do złożenia zlecenia płatniczego umożliwiającego realizację wypłatę środków z salda na rachunek bankowy Partnera lub Klienta oraz inny instrument płatniczy należący do Partnera lub Klienta.
IPN (Instant Product Notification) – komunikat; natychmiastowe powiadomienie wysyłane z Systemu płatności online do Serwisu Partnera przekazujące zmianę statusu

produktu. Struktura IPN jest podobna do ITN (rozszerzona jedynie o węzeł *product* – całość opisane w Dodatku (podrozdział „Natychmiastowe powiadomienia o zmianie statusu produktu (IPN – Instant Product Notification)").

ITN (Instant Transaction Notification) – komunikat; natychmiastowe powiadomienie wysyłane z Systemu płatności online do Serwisu Partnera przekazujące zmianę statusu transakcji.

Karta - karta płatnicza wydana w ramach systemów MOP, dopuszczona regulacjami tychże systemów do realizacji Transakcji bez fizycznej jej obecności.

Klient (Płatnik) – osoba uiszczająca w Serwisie płatność za usługi lub produkty Partnera przy wykorzystaniu Systemu.

Koszyk produktów – jest to informacja o składowych płatności, przekazywana (w Linku płatności) do Systemu w celu późniejszego jej przetwarzania. Każdy produkt koszyka opisują dwa obowiązkowe pola: kwota składowa, oraz pole pozwalające przekazać parametry charakterystyczne dla produktu. Szczegóły w Dodatku (podrozdział „Koszyk produktów") oraz Przykładowe obliczenia wartości funkcji skrótu podczas rozpoczęcia transakcji.

Link płatności – jest żądanie umożliwiające start Transakcji wejściowej, opisane w rozdziale Rozpoczęcie transakcji. Można go stosować w taki sam sposób zarówno w stronach www (metoda POST i GET), jak i w mailach do Klientów (metoda GET).

Marketplace – rozwiązanie płatnicze działające w ramach Systemu Płatności Online BM. Umożliwia Partnerowi obsługę platformy sprzedażowej, na której produkty lub usługi oferowane są Klientom przez Kontrahentów Partnera. Zaawansowane modele rozliczenia Transakcji oraz Transakcji Rozliczeniowych pozwalają na realizację płatności bezpośrednio od Klienta do Kontrahenta Partnera, z jednoczesnym uwzględnieniem Koszyka produktów.

Partner - każdy podmiot, nie będący konsumentem, który jest zainteresowany obsługą przyjmowania przez BM należnych Partnerowi płatności za produkty lub usługi dystrybuowane przez Partnera w Serwisie.

Pay By Link (PBL) – narzędzie umożliwiające realizację płatności za pośrednictwem przelewu wewnątrzbankowego z rachunku Klienta na rachunek BM. Po zalogowaniu się Klienta do bankowości internetowej - dane potrzebne do realizacji przelewu (dane informacyjne odbiorcy, numeru jego rachunku bankowego, kwota i data realizacji przelewu) są wypełnione automatycznie dzięki systemowi wymiany danych pomiędzy bankiem a BM.

Płatność automatyczna – jest to płatność dokonywana, bez potrzeby każdorazowego wprowadzania danych Karty lub danych do autoryzacji przelewu dla innych Instrumentów płatniczych obsługujących płatności automatyczne. Wyróżniamy dwa sposoby zlecania dyspozycji płatności (cyklicznie lub jednym kliknięciem).

Płatność jednym kliknięciem – jest to Płatność automatyczna zlecana przez Klienta.

Płatność cykliczna - jest to Płatność automatyczna zlecana bez udziału Klienta (przez Serwis Partnera).

Rachunek Płatniczy (Saldo) – rachunek płatniczy prowadzony przez BM dla Partnera, na którym gromadzone są środki wpłacone od Klientów.

RecurringAcceptanceState – parametr w komunikatach; określa, czy Klient zaakceptował regulamin płatności automatycznej, czy należy wymusić jego akceptację po stronie Systemu. Dozwolone wartości:

a) NOT_APPLICABLE - nie potrzebna akceptacja regulaminu (płatność jednorazowa kartą lub akcja obciążenia po aktywowaniu usługi, tj. recurringAction o wartości AUTO lub MANUAL),
b) ACCEPTED - akceptacja regulaminu wykonana w serwisie kontrahenta,
c) FORCE - wymagana akceptacja regulaminu, inaczej płatności niemożliwa.

RPAN (Recurring Payment Activation Notification) – komunikat o aktywowaniu usługi płatności automatycznych

RPDN (Recurring Payment Deactivation Notification) – komunikat o dezaktywacji usługi płatności automatycznych

SDK – biblioteka pod najpopularniejsze systemy operacyjne urządzeń mobilnych, ułatwiająca integrację Aplikacji z Systemem. Opis SDK znajduje się w oddzielnym dokumencie.

Serwis – strona lub strony internetowe Partnera zintegrowane z Systemem, na których Klient może nabyć od Partnera produkty lub usługi.

Specyfikacja – niniejszy dokument opisujący komunikację pomiędzy Serwisem a Systemem

System Płatności Online BM (System) – rozwiązanie informatyczno-funkcjonalne, w ramach którego BM udostępnia Partnerowi aplikację informatyczną umożliwiającą przyjmowanie w imieniu i na rzecz Partnera płatności Klientów dokonanych przy użyciu Instrumentów Płatniczych, a także weryfikację statusu płatności oraz odbiór płatności.

Szybki Przelew – realizacja płatności za pośrednictwem przelewu wewnątrzbankowego z rachunku Klienta na rachunek BM. Od płatności dokonywanych za pośrednictwem PBL płatność różni się koniecznością samodzielnego wypełnienia wszystkich danych potrzebnych do dokonania przelewu przez Klienta.

Transakcja - oznacza transakcję płatniczą w rozumieniu Ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych.

Transakcja wejściowa – część procesu obsługi płatności, dotycząca wpłaty dokonywanej przez Klienta do BM.

Transakcja rozliczeniowa – część procesu obsługi płatności, dotycząca przelewu wykonywanego przez BM na rachunek Partnera. Aby powstała Transakcja rozliczeniowa, Transakcja wejściowa musi zostać przez Klienta opłacona. Transakcja rozliczeniowa może dotyczyć pojedynczej transakcji wejściowej (wpłaty), bądź agregować ich wiele.

Ustawa – ustawa z dn. 19 sierpnia 2011 r. o usługach płatniczych.

Ważność linku – parametr określający moment, po przekroczeniu którego Link płatności przestaje być aktywny. Powinna być ustawiana przez parametr LinkValidityTime w Linku płatności.

Ważność transakcji – parametr określający moment, po przekroczeniu którego System płatności online blokuje wpłaty Klienta (są one automatycznie zwracane do Klienta). Wartość domyślna obliczana jest poprzez dodanie 6 dni do momentu wybrania przez Klienta Kanału Płatności. Może ona być również ustawiana przez parametr ValidityTime w Linku płatności. W takim przypadku, po upłynięciu czasu w nim wskazanego, link przestaje być aktywny, a wpłaty są zwracane do Klienta. Maksymalna ważność transakcji to 60 dni (w przypadku ustawienia ValidityTime dalej, niż 60 dni do przodu, czas ważności zostanie odpowiednio skrócony).

Spis treści:

1. Schemat działania usługi

W Serwisie Partnera, po skompletowaniu zamówienia, Klientowi prezentowana jest opcja możliwości wykonania płatności z wykorzystaniem Systemu. Kliknięcie w odpowiedni link powoduje rozpoczęcie transakcji (opisane w punkcie Rozpoczęcie transakcji) i otwarcie w nowym oknie:

a) dedykowanej strony Systemu przygotowanej przez BM, na której Klientowi prezentowana jest lista dostępnych Kanałów Płatności oraz podsumowanie zarejestrowanej transakcji lub
b) bezpośrednio strony Kanału Płatności (Banku, BLIK lub do płatności Kartą).

Po stronie Systemu następuje walidacja przekazanych parametrów i zapisanie transakcji z ustalonym okresem ważności. Jeśli w momencie walidacji, czas ważności linku będzie już przekroczony, Klientowi zostanie wyświetlony odpowiedni komunikat (weryfikacja ważności transakcji następuje także przy zmianie statusu płatności). Po pozytywnej weryfikacji parametrów transakcji (oraz po wybraniu Kanału Płatności), Klient dokonuje autoryzacji transakcji. W jej tytule, oprócz nadawanych przez System identyfikatorów, może być także umieszczany stały opis, ustalony wcześniej pomiędzy BM a Partnerem lub dynamiczna wartość przekazywana przez Partnera przy starcie transakcji.

Zalecany model integracji polega na nadaniu komunikatu rozpoczęcia transakcji „w tle", tzn. bez przekierowania użytkownika do Systemu. W tym modelu, możliwe jest zastosowanie zaawansowanych form autoryzacji transakcji (White Label, płatności automatyczne, SDK mobilne), diagnozowania poprawności przekazywanych parametrów oraz wielu innych rozszerzeń. Szczegóły rozwiązania można znaleźć w Dodatku (1.1 Przedtransakcja).

Po zakończeniu autoryzacji transakcji (na stronie Kanału Płatności) klient powraca z niego do Systemu gdzie następuje automatyczne przekierowanie Klienta do Serwisu Partnera. Szczegółowy opis struktury linku powrotu znajduje się w punkcie Powrót (przekierowanie) na stronę Serwisu Partnera.

Otrzymany z Kanału Płatności status autoryzacji (płatności) przekazywany jest z Systemu do Serwisu Partnera za pomocą komunikatu ITN. System będzie ponawiać wysyłanie komunikatów, aż do potwierdzenia odbioru przez Serwis Partnera lub upłynięcia czasu

ważności powiadomienia. Transakcje, które zostaną zapłacone po opływie okresu ważności transakcji – zostaną zwrócone do Klienta (nadawcy przelewu).

Opcjonalnie System może powiadamiać o fakcie wystawienia Transakcji rozliczeniowej. Służy do tego odpowiednio zmodyfikowany komunikat ISTN – opis w Dodatku („Natychmiastowe powiadomienia o zmianie statusu transakcji rozliczeniowej”).

2. Dane wymieniane podczas integracji

Dane	BM -> Partner	Partner -> BM
Dotyczą środowiska testowego		
Adres Systemu płatności online	X	
ServiceID	X	
(dla portfeli w modelu WhiteLabel) AcceptorID		
Klucz współdzielony	X	
Mechanizm funkcji skrótu	X	
Adres testowego formularza	X	
Adres IP, z którego wysyłane są ITNy	X	
Adres do panelu administracyjnego	X	
Login	X	
Hasło	X	
Adres dla komunikatów ITN		X
(dla płatności automatycznych) Adres dla komunikatów RPAN (może być ten sam adres, co dla komunikatów ITN)		X
(dla płatności automatycznych) Adres dla komunikatów RPDN (może być ten sam adres, co dla komunikatów ITN)		X
Adres powrotu z płatności (bez parametrów)		X
Dotyczą środowiska produkcyjnego		
Adres Systemu płatności online	X	
ServiceID	X	
(dla portfeli w modelu WhiteLabel) AcceptorID		
Klucz współdzielony	X	
Mechanizm funkcji skrótu	X	
Adres IP, z którego wysyłane są ITNy	X	
Adres do panelu administracyjnego	X	
Login	X	
Hasło	X	
Adres dla komunikatów ITN		X
(dla płatności automatycznych) Adres dla komunikatów RPAN (może być ten sam adres, co dla komunikatów ITN)		X

(dla płatności automatycznych) Adres dla komunikatów RPDN (może być ten sam adres, co dla komunikatów ITN)		X
Adres powrotu z płatności (bez parametrów)		X
Adresy email dla raportów transakcyjnych		X
Adresy email dla faktur i raportów rozliczeniowych		X
Adresy email dla reklamacji (wysyłany w wiadomościach do płatników)		X
Informacje ogólne		
Aktywne Kanały Płatności wraz z grafikami (Dodatek: „Odpytywanie o listę aktualnie dostępnych Kanałów Płatności”)	X	
Opcjonalnie: informacje o wymaganej zawartości koszyka i sposobie przetwarzania go (np. w raportach, rozliczeniach, panelu administracyjnym), dodatkowe wymagania (np. na zasilenia salda przedpłaconego)		X

3. Rozpoczęcie transakcji

Serwis Partnera inicjując transakcję przekazuje do Systemu płatności online parametry niezbędne do jej zrealizowania oraz późniejszego przekazania statusu płatności. Wszystkie parametry przekazywane są metodą GET lub POST (Content-Type: application/x-www-form-urlencoded). Protokół rozróżnia wielkość liter zarówno w nazwach jak i wartościach parametrów. Wartości przekazywanych parametrów powinny być kodowane w UTF-8 (oraz protokołem transportowym[1]). Poniżej lista dostępnych parametrów:

Kolejność do Hash	Nazwa	Wymagany	Typ	Opis
1	**ServiceID**	**TAK**	string{1,10}[2]	Identyfikator Serwisu Partnera, nadawany w trakcie rejestracji usługi, jednoznacznie identyfikuje Serwis Partnera w Systemie płatności online.
2	**OrderID**	**TAK**	string{1,32}[3]	Identyfikator transakcji o długości do 32 znaków alfanumerycznych alfabetu łacińskiego. Wartość pola musi być unikalna dla Serwisu Partnera.
3	**Amount**	**TAK**	amount	Kwota transakcji. Jako separator dziesiętny używana jest kropka - '.' Format: 0.00; maksymalna długość: 14 cyfr przed kropką i 2 po kropce. Uwaga: Dopuszczalna wartość pojedynczej Transakcji w Systemie produkcyjnym wynosi odpowiednio[4]: - dla PBL - min. 0.01 PLN, max. 100000.00 PLN (lub do wysokości ustalonej przez Bank wydający instrument płatniczy)

[1] Zakodować przed wysłaniem, o ile narzędzie wykorzystane do wysyłki komunikatu nie robi tego samodzielnie, przykład kodowania: URLEncode

[2] Dopuszczalne cyfry

[3] Dopuszczalne alfanumeryczne znaki alfabetu łacińskiego oraz znaki z zakresu: -_

[4] Jeśli prowizja za transakcję jest pobierana z kwoty rozliczenia z Partnerem i jest ona płaska, to wartość ta staje się minimalną wartością Transakcji w Systemie

				- dla Kart płatniczych – min. 0.10 PLN, max. 100000.00 PLN (lub do wysokości indywidualnego limitu pojedynczej transakcji w Banku wydawcy Karty) - dla Szybkich przelewów - min. 0.01 PLN, max. 100000.00 PLN (lub do wysokości indywidualnego limitu pojedynczej transakcji w Banku dla przelewu wewnątrzbankowego) - dla BLIK - min. 0.01 PLN, max. 75000.00 PLN (lub do wysokości indywidualnego limitu pojedynczej transakcji w Banku dla przelewu wewnątrzbankowego).
4	**Description**	NIE	string{1,79}[5]	Tytuł transakcji (wpłaty); na początku tytułu przelewu umieszczane są identyfikatory transakcji nadawane przez System płatności online, do tego doklejana jest wartość tego parametru. W niektórych przypadkach, niezależnych od BM tytuł przelewu może zostać dodatkowo zmodyfikowany przez Bank, w którym nastąpiła wpłata dokonana przez klienta.
5	**GatewayID**	NIE	integer{1,5}	Identyfikator Kanału Płatności, za pomocą, którego Klient zamierza uregulować płatność. Ten parametr odpowiada w szczególności za model prezentowania Kanałów Płatności: - na stronie BM – wartość parametru „0” - w Serwisie Partnera – wartość parametru odpowiada wybranemu przez Klienta Kanałowi Płatności np. GatewayID=3. Wszystkie Kanały Płatności do samodzielnego osadzenia w Serwisie udostępniane są Partnerowi w ramach usługi gatewayList (opis w Dodatku).
6	**Currency**	NIE	string{1,3}[6]	Waluta transakcji; domyślną walutą jest PLN (użycie innej waluty musi być uzgodnione w

[5] Dopuszczalne alfanumeryczne znaki alfabetu łacińskiego oraz znaki z zakresu: . : / - , spacja
[6] Dopuszczalne jedynie wartości: PLN, EUR, GBP oraz USD.

				trakcie integracji); w ramach ServiceID obsługiwana jest jedna waluta.
7	**CustomerEmail**	NIE	string{3,255}	Adres email Klienta.
19	**ValidityTime**	NIE	string{1,19}	Moment upłynięcia ważności transakcji; po jego przekroczeniu link przestaje być aktywny, a wszelkie wpłaty są zwracane do nadawcy przelewu; przykładowa wartość: 2014-10-31 07:54:50; w przypadku braku parametru ustawiana jest wartość domyślna 6 dni. Maksymalna ważność transakcji to 60 dni (w przypadku ustawienia wartości parametru dalej, niż 60 dni do przodu, czas ważności zostanie odpowiednio skrócony). Przykładowo transakcja wystartowana w chwili 2020-05-01 08:00:00, z parametrem ValidityTime = 2021-05-01 08:00:00, otrzyma ważność do chwili 2020-06-29 08:00:00.
34	**LinkValidityTime**	NIE	string{1,19}	Moment upłynięcia ważności linku; po jego przekroczeniu link przestaje być aktywny, nie wpływa to jednak na czas oczekiwania na wpłatę; przykładowa wartość: 2014-10-30 07:54:50; proszę zwrócić uwagę na to, aby do czasu ważności linku, dostosowany był czas ważności transakcji (być może zajdzie potrzeba podania również parametru ValidityTime, aby wydłużyć jej standardową ważność).
nd.	**Hash**	**TAK**	string{1,128}	Wartość funkcji skrótu dla komunikatu obliczona zgodnie z opisem w rozdziale Bezpieczeństwo.

Rozpoczęcie transakcji następuje przez przesłanie wywołaniem HTTPS, kombinacji powyższych parametrów, na ustalony w trakcie rejestracji usługi, adres Systemu płatności online. Przykładowe rozpoczęcie transakcji ma postać:

https://host_bramki/sciezka?ServiceID=2&OrderID=100&Amount=1.50&Hash=2ab52e6918c6ad3b69a8228a2ab815f11ad58533eeed963dd990df8d8c3709d1

Przesłanie komunikatu bez wszystkich **wymaganych** parametrów (**ServiceID, OrderID, Amount i Hash**) lub zawierającego błędne ich wartości, spowoduje zatrzymanie procesu płatności wraz z podaniem kodu błędu transakcji i krótką informacją o błędzie (brak powrotu na stronę Serwisu Partnera).

Para parametrów **ServiceID** i **OrderID** jednoznacznie identyfikuje transakcję. Niedopuszczalne jest powtórzenie się wartości parametru OrderID przez cały okres świadczenia usług przez System na rzecz jednego Serwisu Partnera (ServiceID).

Opcjonalny parametr GatewayID służy do określenia Kanału Płatności, za pomocą którego ma zostać zrealizowana płatność. Pozwala to przenieść ekran wyboru Kanałów Płatności do Serwisu. Aktualna lista identyfikatorów Kanałów Płatności, wraz z logotypami, dostępna jest poprzez metodę gatewayList (Dodatek: „Odpytywanie o listę aktualnie dostępnych Kanałów Płatności").

Komunikat rozpoczęcia transakcji może być nadany w tle, tzn. bez przekierowania użytkownika do Systemu płatności online. W tym modelu, samego wyboru Kanału Płatności, Klient także dokonuje w Serwisie Partnera. Szczegóły tego rozwiązania zostały opisane w Dodatku (punkt „Przedtransakcja" oraz „Zamówienie danych do przelewu w transakcji typu Szybki Przelew").

4. Powrót (przekierowanie) na stronę Serwisu Partnera

Niezwłocznie po zakończeniu autoryzacji transakcji przez Klienta jest on przekierowywany z witryny Kanału Płatności na witrynę Systemu płatności online gdzie następuje automatyczne przekierowanie Klienta do Serwisu Partnera. Przekierowanie realizowane jest poprzez wysłanie żądania HTTPS (metodą GET) pod ustalony wcześniej adres powrotu w Serwisie Partnera. Protokół rozróżnia wielkość liter zarówno w nazwach jak i wartościach parametrów. Poniżej lista dostępnych parametrów:

Kolejność do HASH	Nazwa	Wymagany	Typ	Opis
1	**ServiceID**	TAK	string{1,10}	Identyfikator Serwisu Partnera.
2	**OrderID**	TAK	string{1,32}	Identyfikator transakcji nadany w Serwisie Partnera i przekazany w starcie transakcji.
nd.	**Hash**	TAK	string{1,128}	Wartość funkcji skrótu dla komunikatu obliczona zgodnie z opisem w rozdziale Bezpieczeństwo. **Weryfikacja zgodności wyliczonego skrótu przez Serwis Partnera jest obowiązkowa.**

Przykładowy komunikat, przekierowujący Klienta z Systemu płatności online do Serwisu Partnera:

https://sklep_nazwa/strona_powrotu?ServiceID=2&OrderID=100&Hash=254eac9980db56f425acf8a9df715cbd6f56de3c410b05f05016630f7d30a4ed

5. Natychmiastowe powiadomienia o zmianie statusu transakcji wejściowej (ITN – Instant Transaction Notification)

System przekazuje powiadomienia o zmianie statusu transakcji niezwłocznie po otrzymaniu takiej informacji z Kanału Płatności (komunikat zawsze dotyczy pojedynczej transakcji). Potwierdzenia przesyłane są przez System płatności online, na ustalony w trakcie dodawania konfiguracji Serwisu Partnera, adres na serwerze Serwisu Partnera (Uwaga: domena musi być publiczna i dostępna przez System):

https://sklep_nazwa/odbior_statusu

Powiadomienie o zmianie statusu transakcji wejściowej polega na wysłaniu przez System dokumentu XML zawierającego nowe statusy transakcji. Dokument wysyłany jest protokołem HTTPS, ew. HTTP (dozwolone porty 80 i 443). Dokument przesyłany jest metodą POST, jako parametr HTTP o nazwie transactions. Parametr ten zapisany jest mechanizmem kodowania transportowego Base64. Format dokumentu jest następujący:

```
<?xml version="1.0" encoding="UTF-8"?>
<transactionList>
        <serviceID>ServiceID</serviceID>
        <transactions>
                <transaction>
                        <orderID>OrderID</orderID>
                        <remoteID>RemoteID</remoteID>
                        <amount>999999.99</amount>
                        <currency>PLN</currency>
                        <gatewayID>GatewayID</gatewayID>
                        <paymentDate>YYYYMMDDhhmmss</paymentDate>
                        <paymentStatus>PaymentStatus</paymentStatus>
                        <paymentStatusDetails>PaymentStatusDetails</paymentStatusDet
                        ails>
                </transaction>
        </transactions>
        <hash>Hash</hash>
</transactionList>
```

Węzeł transactions może zawierać jedynie jeden węzeł transaction (a więc powiadomienie dotyczy zawsze jednej transakcji). Wartości elementów: orderID, amount dotyczące każdej z transakcji, są identyczne z wartościami odpowiadających im pól, podanymi przez Serwis Partnera przy rozpoczęciu danej transakcji. Poniżej opis zwracanych parametrów:

Kolejność do Hash	Nazwa	Wymagany	Typ	Opis
1	**serviceID**	TAK	string{1,10}	Identyfikator Serwisu Partnera, nadawany w trakcie rejestracji usługi, jednoznacznie identyfikuje Serwis Partnera w Systemie płatności online.
2	**orderID**	TAK	string{1,32}	Identyfikator transakcji nadany w Serwisie Partnera i przekazany w starcie transakcji.
3	**remoteID**	TAK	string{1,20}	Alfanumeryczny identyfikator transakcji nadany przez System płatności online. Warto go zapisać przy zamówieniu na potrzeby dalszej obsługi (wielu transakcji z tym samym OrderID[7] – opis niżej, zwrotów – opis w Dodatku, itp.).
5	**amount**	TAK	amount	Kwota transakcji, jako separator dziesiętny używana jest kropka - '.' Format: 0.00; maksymalna długość: 14 cyfr przed kropką i 2 po kropce.
6	**currency**	TAK	string{1,3}	Waluta transakcji.
7	**gatewayID**	NIE	string{1,5}	Identyfikator Kanału Płatności, za pomocą, którego Klient uregulował płatność.
8	**paymentDate**	TAK	string{14}	Moment zautoryzowania transakcji, przekazywany w formacie YYYYMMDDhhmmss.
9	**paymentStatus**	TAK	enum	Status autoryzacji transakcji, przyjmuje wartości (opis zmian statusów dalej): **PENDING** – transakcja rozpoczęta. **SUCCESS** – poprawna autoryzacja transakcji, Serwis Partnera otrzyma środki za transakcje - można wydać towar/usługę.

[7] Sytuacja taka może mieć miejsce np. w przypadku gdy Klient zmieni Kanał Płatności, wywoła ponownie ten sam start transakcji z historii przeglądarki itp. System umożliwia blokowanie takich przypadków, jednak opcja nie jest zalecana (nie byłoby możliwe opłacenie porzuconej transakcji).

				FAILURE – transakcja nie została zakończona poprawnie.
10	**paymentStatusDetails**	NIE	string{1,64}	Szczegółowy status transakcji, wartość może być ignorowana przez Serwis Partnera. Opis pola w Dodatku (rozdział „Szczegółowe statusy transakcji”).
nd.	**hash**	TAK	string{1,128}	Wartość funkcji skrótu dla komunikatu obliczona zgodnie z opisem w rozdziale Bezpieczeństwo. **Weryfikacja zgodności wyliczonego skrótu przez Serwis Partnera jest obowiązkowa.**

Element hash (komunikatu) służy do autentykacji dokumentu. Opis sposobu obliczania skrótu znajduje się w rozdziale Bezpieczeństwo.

W odpowiedzi na powiadomienie oczekiwany jest status HTTP 200 (OK) oraz tekst w formacie XML (nie kodowany Base64), zwracany przez Serwis Partnera w tej samej sesji HTTP, zawierający potwierdzenie otrzymania statusu transakcji. Struktura potwierdzenia jest następująca:

```
<?xml version="1.0" encoding="UTF-8"?>
<confirmationList>
        <serviceID>ServiceID</serviceID>
        <transactionsConfirmations>
                <transactionConfirmed>
                        <orderID>OrderID</orderID>
                        <confirmation>Confirmation</confirmation>
                </transactionConfirmed>
        </transactionsConfirmations>
        <hash>Hash</hash>
</confirmationList>
```

Poniżej opis tych pól:

Kolejność do HASH	Nazwa	Wymagany	Typ	Opis
1	**serviceID**	TAK	string{1,10}	Identyfikator Serwisu Partnera. Pochodzi z komunikatu.

2	**orderID**	TAK	string{32}	Identyfikator transakcji nadany w Serwisie Partnera i przekazany w starcie transakcji. Pochodzi z komunikatu.
3	**confirmation**	TAK	string{1,25}	Element służy do przekazania stanu weryfikacji autentyczności transakcji przez Serwis Partnera. Wartość elementu wyznaczana jest przez sprawdzenie poprawności wartości parametru serviceID oraz currency, porównanie wartości pól orderID i amount w komunikacie powiadomienia oraz w komunikacie rozpoczynającym transakcję, a także weryfikację zgodności wyliczonego skrótu z parametrów komunikatu z wartością przekazaną w polu hash komunikatu. Przewidziano dwie wartości elementu confirmation: **CONFIRMED** – wartości parametrów w obu komunikatach oraz parametr hash są zgodne – transakcja autentyczna; **NOTCONFIRMED** – wartości w obu komunikatach są różne lub niezgodność hash – transakcja nieautentyczna;
nd.	**hash**	TAK	string{1,128}	Element hash (w odpowiedzi na komunikat) służy do autentykacji odpowiedzi i liczony jest z wartości parametrów odpowiedzi. Opis sposobu obliczania skrótu znajduje się w rozdziale Bezpieczeństwo.

W wypadku braku poprawnej odpowiedzi na wysłane powiadomienia, System podejmie kolejne próby przekazania najnowszego statusu transakcji po upływie określonego czasu. Serwis Partnera powinien wykonywać własną logikę biznesową (np. mail z potwierdzeniem), jedynie po pierwszym komunikacie o danym statusie płatności. Schemat opisujący planowe ponawianie ITN w Dodatku: „Schemat ponawiania komunikatów ITN/ISTN/IPN/RPAN/RPDN". Zaleca się również zapoznanie z rozdziałem Dodatku „Monitoring komunikacji ITN/ISTN/IPN/RPAN/RPDN".

5.1 Szczegółowy opis zachowania i zmiany statusów płatności (paymentStatus)

Rezygnacja/powrót Klienta z ekranu listy metod płatności (bez dokonania wyboru), spowoduje od razu wysłanie statusu **FAILURE** (status **PENDING** nigdy wystąpi, gdyż Klient tak naprawdę nie rozpoczął płatności).
Wybór przez Klienta metody płatności każdorazowo spowoduje wysłanie statusu **PENDING**. W kolejnym komunikacie ITN system dostarczy status **SUCCESS** lub **FAILURE**.

Dla pojedynczej transakcji (o unikatowych parametrach OrderID oraz RemoteID) nie może nastąpić zmiana statusu **SUCCESS** na **PENDING** lub **SUCCESS** na **FAILURE**.
W każdym przypadku może nastąpić zmiana statusu szczegółowego – paymentStatusDetails (kolejne komunikaty o zmianie statusu szczegółowego są jedynie informacyjne i nie powinny prowadzić do ponownego wykonania opłacanej usługi/wysyłki produktu itp.).

W szczególnych przypadkach użycia może nastąpić zmiana statusu:

a) **FAILURE** na **SUCCESS** (np. po zatwierdzeniu przez konsultanta BM transakcji wpłaconej z błędną kwotą. Takie zachowania wymaga specjalnych uzgodnień biznesowych i nie jest włączone domyślnie),
b) **SUCCESS** na **FAILURE** (np. po wywołaniu wielu transakcji z tym samym OrderID, ale różnym RemoteID). Taki przypadek występuje w sytuacji rozpoczęcia przez Klienta wielu płatności z tym samym OrderID (np. Klient zmienia decyzję, jakim Kanałem płatności chce opłacić transakcję). Każda z rozpoczętych przez niego płatności generuje ITNy i poszczególne transakcje Partner powinien rozróżnić na podstawie parametru RemoteID. Ponieważ czas otrzymania statusu **FAILURE** może być bardzo różny, może się zdarzyć otrzymanie takiego statusu po odebraniu **SUCCESS** (oczywiście z innym RemoteID). W takim wypadku, komunikat ITN powinien być potwierdzany, ale nie powinien pociągać za sobą anulowania statusu transakcji w systemie Partnera.

Obsługa statusów transakcji z ITN – model uproszczony

W modelu, w którym nie jest potrzebne powiadamianie mailem/smsem Klienta o statusach innych niż SUCCESS, można ograniczyć ilość informacji zapisywanych do bazy Serwisu oraz śledzenie zmian RemoteID. Wystarczy jedynie:

- dla statusów innych niż SUCCESS, za każdym razem potwierdzać ITN poprawną strukturą odpowiedzi, statusem CONFIRMED oraz poprawnie policzoną wartością pola Hash,
- w przypadku otrzymania **pierwszego** statusu SUCCESS, dodać również aktualizację statusu, jego czasu i RemoteID w bazie Serwisu oraz realizację procesów biznesowych (powiadomienia do Klienta o zmianie statusu, wykonania opłacanej usługi/wysyłki produktu itp.),
- w przypadku otrzymania kolejnego statusu SUCCESS, za każdym razem potwierdzać ITN poprawną strukturą odpowiedzi, statusem CONFIRMED oraz poprawnie policzoną wartością pola Hash, bez aktualizacji bazy Serwisu oraz bez procesów biznesowych.

Obsługa statusów transakcji z ITN – model pełny

W modelu, w którym potrzebna jest cała historia zmian statusów transakcji i/lub powiadamianie Klienta o ważniejszych zmianach statusów transakcji należy zastosować logikę przybliżoną do poniższego opisu.

Dotychczasowy ogólny Status Płatności	PaymentStatus w ITN	Różne RemoteID	Proces biznesowy (powiadomienia do Klienta o zmianie statusu)	Proces biznesowy (wykonanie opłacanej usługi/wysyłki produktu itp.)	Zawartość pola confirmation odpowiedzi	Aktualizacja ogólnego statusu transakcji, jej czasu i wartości RemoteID	Uwagi
Brak	Pending	Nd	Tak	Nie	CONFIRMED	Tak	
Brak	Failure	Nd	Tak	Nie	CONFIRMED	Tak	
Brak	Sucess	Nd	Tak	Tak	CONFIRMED	Tak	
Pending	Pending	Nie	Nie	Nie	CONFIRMED	Nie	
Pending	Failure	Nie	Tak	Nie	CONFIRMED	Tak	
Pending	Sucess	Nie	Tak	Tak	CONFIRMED	Tak	
Failure	Pending	Nie	Nie	Nie	CONFIRMED	Nie	
Failure	Failure	Nie	Nie	Nie	CONFIRMED	Nie	
Failure	Sucess	Nie	Tak	Tak	CONFIRMED	Tak	
Sucess	Pending	Nie	Nie	Nie	CONFIRMED	Nie	Niemożliwe
Sucess	Failure	Nie	Nie	Nie	CONFIRMED	Nie	Niemożliwe
Sucess	Sucess	Nie	Nie	Nie	CONFIRMED	Nie	
Pending	Pending	Tak	Nie	Nie	CONFIRMED	Nie	
Pending	Failure	Tak	Tak	Nie	CONFIRMED	Tak	
Pending	Sucess	Tak	Tak	Tak	CONFIRMED	Tak	
Failure	Pending	Tak	Nie	Nie	CONFIRMED	Tak	
Failure	Failure	Tak	Nie	Nie	CONFIRMED	Nie	
Failure	Sucess	Tak	Tak	Tak	CONFIRMED	Tak	
Sucess	Pending	Tak	Nie	Nie	CONFIRMED	Nie	Niemożliwe
Sucess	Failure	Tak	Nie	Nie	CONFIRMED	Nie	Niemożliwe
Sucess	Sucess	Tak	Nie	Nie	NOTCONFIRMED	Nie	Niemożliwe

6. Bezpieczeństwo transakcji

W Systemie płatności online zastosowano kilka mechanizmów zwiększających bezpieczeństwo realizowanych przy jego użyciu transakcji. Transmisja między wszystkimi stronami transakcji realizowana jest w oparciu o bezpieczne połączenie oparte na protokole TLS z 256 bitowym kluczem. Dodatkowo, komunikacja zabezpieczana jest funkcją skrótu obliczoną z wartości pól komunikatu i współdzielonego klucza. Jako funkcja skrótu wykorzystywany jest algorytm MD5, SHA-1, SHA256 lub SHA512 (metoda ustalana na etapie konfigurowania danego Serwisu Partnera w Systemie płatności online). Domyślna funkcja to SHA256. Poniżej opis sposobu obliczania wartości funkcji skrótu oraz przykłady obliczeń dla podstawowych komunikatów.

UWAGA! Przykłady nie uwzględniają wszystkich możliwych pól opcjonalnych, dlatego w razie występowania takich pól w konkretnym komunikacie, należy uwzględnić je w funkcji skrótu zgodnie z kolumną 'Kolejność do Hash'.

6.1 Sposób obliczania wartości funkcji skrótu – pole Hash

Wartość funkcji skrótu, służąca do autentykacji komunikatu, obliczana jest od łańcucha zawierającego sklejone pola komunikatu (konkatenacja pól). Sklejane są wartości pól, bez nazw parametrów, a pomiędzy kolejnymi (niepustymi) wartościami wstawiany jest separator (w postaci znaku |). Kolejność sklejania pól jest zgodna z kolejnością ich występowania na liście parametrów w niniejszym dokumencie (kolumna 'Kolejność do Hash').

UWAGA! W przypadku braku opcjonalnego parametru w komunikacie lub w przypadku pustej wartości parametru, nie należy używać separatora!

Do powstałego w powyższy sposób łańcucha doklejany jest na jego końcu klucz, współdzielony między Serwis Partnera i System płatności online. Z tak powstałego łańcucha obliczana jest wartość funkcji skrótu i stanowi ona wartość pola Hash komunikatu.

Hash = funkcja(wartości_pola_1_komunikatu + "|" + wartości_pola_2_komunikatu + "|" + … + "|" + wartości_pola_n_komunikatu + "|" + klucz_współdzielony);

6.2 Przykładowe obliczenia wartości funkcji skrótu podczas rozpoczęcia transakcji

a. Dane Serwisu Partnera bez koszyka:

ServiceID = 2
klucz_współdzielony = 2test2

Rozpoczęcie transakcji, wywołanie GET:

https://host_bramki/sciezka?ServiceID=2&OrderID=100&Amount=1.50&
Hash=2ab52e6918c6ad3b69a8228a2ab815f11ad58533eeed963dd990df8d8c3709d1

gdzie wartość
Hash=SHA256("2|100|1.50|2test2")

b. Dane Serwisu Partnera z koszykiem – opcja opisana w Dodatku (podrozdział „Koszyk produktów"):

ServiceID = 2
OrderID = 100
Amount = 1.50
klucz_współdzielony = 2test2

Koszyk produktów:
<?xml version="1.0" encoding="UTF-
8"?><productList><product><subAmount>1.00</subAmount><params><param
name="productName" value="Nazwa produktu 1"
/></params></product><product><subAmount>0.50</subAmount><params><param
name="productType" value="ABCD" /><param name="ID" value="EFGH"
/></params></product></productList>

Po zakodowaniu funkcją base64 otrzymujemy wartość parametru Product:
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48cHJvZHVjdExpc3Q+PHByb
2R1Y3Q+PHN1YkFtb3VudD4xLjAwPC9zdWJBbW91bnQ+PHBhcmFtcz48cGFyYW0gbmFtZT
0icHJvZHVjdE5hbWUiIHZhbHVlPSJOYXp3YSBwcm9kdWt0dSAxIiAvPjwvcGFyYW1zPjwvcHJ
vZHVjdD48cHJvZHVjdD48c3ViQW1vdW50PjAuNTA8L3N1YkFtb3VudD48cGFyYW1zPjxwYX
JhbSBuYW1lPSJwcm9kdWN0VHlwZSIgdmFsdWU9IkFCQ0QiIC8+PHBhcmFtIG5hbWU9IklE
IiB2YWx1ZT0iRUZHSCIgLz48L3BhcmFtcz48L3Byb2R1Y3Q+PC9wcm9kdWN0TGlzdD4=

Wartość Hash liczona jest w następujący sposób:

Hash=SHA256(“2|100|1.50|PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48cHJvZHVjdExpc3Q+PHByb2R1Y3Q+PHN1YkFtb3VudD4xLjAwPC9zdWJBbW91bnQ+PHBhcmFtcz48cGFyYW0gbmFtZT0icHJvZHVjdE5hbWUiIHZhbHVlPSJOYXp3YSBwcm9kdWt0dSAxIiAvPjwvcGFyYW1zPjwvcHJvZHVjdD48cHJvZHVjdD48c3ViQW1vdW50PjAuNTA8L3N1YkFtb3VudD48cGFyYW1zPjxwYXJhbSBuYW1lPSJwcm9kdWN0VHlwZSIgdmFsdWU9IkFCQ0QiIC8+PHBhcmFtIG5hbWU9IklEIiB2YWx1ZT0iRUZHSCIgLz48L3BhcmFtcz48L3Byb2R1Y3Q+PC9wcm9kdWN0TGlzdD4=|2test2”)

6.3 Przykładowe obliczenia wartości funkcji skrótu podczas powrotu Klienta do Serwisu Partnera

Dane Serwisu Partnera:
ServiceID = 2
klucz_współdzielony = 2test2

https://sklep_nazwa/strona_powrotu?ServiceID=2&OrderID=100&Hash=254eac9980db56f425acf8a9df715cbd6f56de3c410b05f05016630f7d30a4ed

gdzie wartość
Hash=SHA256(“2|100|2test2”)

6.4 Przykładowe obliczenia wartości funkcji skrótu w komunikacie ITN

Dane Serwisu Partnera:
serviceID = 1
klucz_współdzielony = 1test1

ITN:

```
<?xml version="1.0" encoding="UTF-8"?>
<transactionList>
        <serviceID>1</serviceID>
        <transactions>
                <transaction>
                        <orderID>11</orderID>
                        <remoteID>91</remoteID>
```

```
                    <amount>11.11</amount>
                    <currency>PLN</currency>
                    <gatewayID>1</gatewayID>
                    <paymentDate>20010101111111</paymentDate
                    <paymentStatus>SUCCESS</paymentStatus>
                    <paymentStatusDetails>AUTHORIZED</paymentStatusDetails>
            </transaction>
        </transactions>
        <hash>a103bfe581a938e9ad78238cfc674ffafdd6ec70cb6825e7ed5c41787671efe
        4</hash>
</transactionList>
```

gdzie wartość
Hash=SHA256(“1|11|91|11.11|PLN|1|20010101111111|SUCCESS|AUTHORIZED|1test1”
)

Odpowiedź na powyższe wywołanie może być następujące:

```
<?xml version="1.0" encoding="UTF-8"?>
<confirmationList>
        <serviceID>1</serviceID>
        <transactionsConfirmations>
                <transactionConfirmed>
                        <orderID>11</orderID>
                        <confirmation>CONFIRMED</confirmation>
                </transactionConfirmed>
        </transactionsConfirmations>
        <hash>c1e9888b7d9fb988a4aae0dfbff6d8092fc9581e22e02f335367dd01058f961
        8</hash>
</confirmationList>
```

gdzie wartość
Hash=SHA256(“1|11|CONFIRMED|1test1”);

6.5 Przykładowe obliczenia wartości funkcji skrótu w odpytaniu o listę Kanałów Płatności

Usługa opisana w Dodatku (podrozdział „Odpytywanie o listę aktualnie dostępnych Kanałów Płatności”).
Dane Serwisu Partnera:
serviceID = 1
messageID = cfb91538ad854d74813ea76893cc020c
klucz_współdzielony = 1test1

gdzie wartość
Hash=SHA256(“1|cfb91538ad854d74813ea76893cc020c|1test1”);

Odpowiedź na powyższe wywołanie może być następująca:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<list>
  <serviceID>1</serviceID>
  <messageID>cfb91538ad854d74813ea76893cc020c</messageID>
  <gateway>
    <gatewayID>19</gatewayID>
    <gatewayName>Przelew PKOBP</gatewayName>
    <gatewayType>Szybki Przelew</gatewayType>
    <bankName>INTELIGO</bankName>
    <iconURL>https://host/sciezka/19.png</iconURL>
    <statusDate>2015-10-14 12:12:31</statusDate>
  </gateway>
  <gateway>
    <gatewayID>106</gatewayID>
    <gatewayName>platnosc testowa PG</gatewayName>
    <gatewayType>PBL</gatewayType>
    <bankName>NONE</bankName>
    <statusDate>2015-10-14 12:12:31</statusDate>
  </gateway>
  <hash>
3e344203abf12631ad88a20c60119ff42e7d892f75d148293d4e7938ba18e794</hash>
</list>
```

gdzie wartość

Hash=SHA256("1|cfb91538ad854d74813ea76893cc020c|19|Przelew PKOBP|Szybki Przelew|INTELIGO|https://host /sciezka/19.png|2015-10-14 12:12:31|106|platnosc testowa PG|PBL|NONE|2015-10-14 12:12:31|1test1");