Dokumentacja usługi weryfikacji - ID HUB

Data wygenerowania: 2021-11-23

Specyfikacja integracji

Wersja dokumentu -1.9

Definicje

ID HUB (Usługa, System) – opisywane narzędzie. Zorganizowany zbiór mechanizmów służących do oceny przez Partnera prawdziwości danych Klienta. Weryfikacja może obejmować dane osobowe, zgodność wizerunku z dokumentem czy zdolność kredytową.

Klient – użytkownik docelowy, osoba korzystająca z usługi, dokonująca uwierzytelnienia swoich danych.

Partner – kontrahent, podmiot integrujący się z ID HUB (administrator strony/platformy technologicznej z której korzysta Klient).

Paywall – widok w interfejsie, na którym prezentowana jest Klientowi lista dostępnych banków/kanałów płatności, którymi może zrealizować usługę.

Komponent – element składowy usługi dostarczający mechanizm weryfikacji w określonym dla Partnera zakresie (np. weryfikacja imienia i nazwiska na podstawie danych z rachunku bankowego).

Raport / Raport dzienny / Raport miesięczny – wysyłany do Partnera dokument z danymi dotyczącymi ilości transakcji wykonanych w określonym czasie.

Weryfikacja – proces technologiczny polegający na przyjęciu przez System danych Klienta oraz przekazaniu informacji zwrotnej określonej przez dany Komponent (np. foto-weryfikacja zdjęć, dane rachunku bankowego).

Wynik weryfikacji – dokument wytworzony przez Komponent weryfikacyjny. Może zawierać status i/lub dane dodatkowe. Jego treść jest specyficzna dla danego Komponentu.

Narzędzie ID HUB

ID HUB to narzędzie umożliwiające zbadanie przez Partnera wiarygodności swojego Klienta lub pobrania danych osobowych Klienta i danych o kliencie z zewnętrznych źródeł (dokumenty, rachunki bankowe, bazy gospodarcze).

Weryfikacja i pozyskanie danych mogą być wykonane przez różne komponenty, każdy z nich o odmiennej charakterystyce.

Możliwości narzędzia to:

1. mechanizm skanowania rachunków bankowych przy pomocy interfejsów PSD2 i realizacja przelewu na jedną złotówkę i weryfikacja danych transakcji
2. fotoweryfikacja - OCR dowodu osobistego
3. fotoweryfikacja - OCR dowodu osobistego i weryfikacja biometryczna Klienta

ID HUB unifikuje wszystkie komponenty w jeden interfejs i standaryzuje sposób przeprowadzenia

Klienta przez proces – niezależnie od tego, do jakiego rodzaju procedury weryfikacji/dostarczenia danych Partner zobowiązuje swoich Klientów.

Sposób działania usługi ID HUB

Klient w systemie Partnera wykonuje akcję wymagającą zweryfikowania jego tożsamości. Partner wysyła do Systemu żądanie utworzenia nowej Weryfikacji. ID HUB, na bazie konfiguracji konta Partnera, analizuje jakiego rodzaju Weryfikacja powinna być wykonana. Jeśli System dysponuje Komponentem, który ma możliwość zweryfikowania określonych przez Partnera parametrów, kontaktuje się z nim i buduje unikalny adres URL, na który należy przekierować Klienta.

Adres URL jest zwracany do systemu Partnera razem z identyfikatorem nadanym nowej Weryfikacji. System Partnera w odpowiednim momencie przekierowuje Klienta na otrzymany adres. Klient przechodzi do witryny w domenie Blue Media lub bezpośrednio do banku i postępuje według kroków wyznaczanych przez wybrany Komponent weryfikacyjny. Po wykonaniu wszystkich akcji, jakich zażądał Komponent, Klient jest przekierowywany z powrotem do systemu Partnera. W tym momencie Wynik weryfikacji powinien być już dostępny dla systemu Partnera.

Wynik zakończonej weryfikacji Partner pobiera wysyłając żądanie na ustalony, opisany w dalszej części dokumentu adres. W odpowiedzi System zwróci obliczony wynik weryfikacji albo informację, że ten jest w trakcie przygotowywania. Do samego wyniku, poszczególne komponenty mogą dołączyć dodatkowe dane – tzw. raporty. Treści raportów są specyficzne dla wybranych komponentów.

Jest możliwość, aby to System aktywnie powiadamiał Partnera o przygotowanym wyniku weryfikacji. Jest to tzw. PUSH. Wymaga on dostarczenia przez system Partnera adresu URL, który HUB będzie wywoływał, dostarczając notyfikację o możliwości pobrania gotowego wyniku.

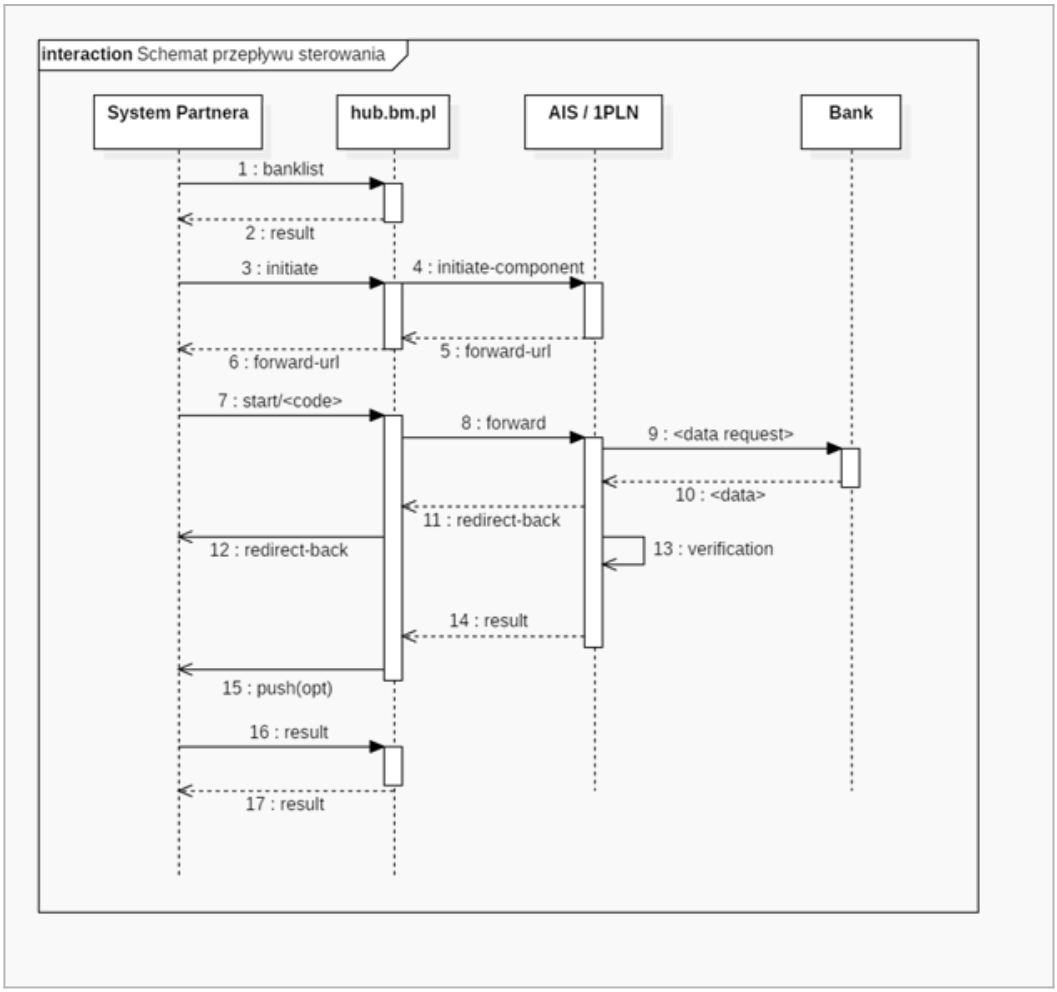

Diagram sekwencji

Procedura integracji ID HUB

Integracja dla nowego Partnera

Integracja z Systemem weryfikacji składa się z następujących kroków:

1. Ustalenie z Opiekunem Biznesowym parametrów działania systemu. W kroku tym Partner określa swoje potrzeby, definiuje wymagania względem ID HUBa. Wybierane są niezbędne komponenty oraz parametry ich używania. Rezultatem tego kroku jest wypełniony dokument karty wdrożeniowej.
2. Na podstawie wypełnionej karty, w środowisku testowym tworzone jest konto.
3. Partner może skorzystać z aplikacji: https://id-hub-accept.bm.pl/test/start

WSKAZÓWKA: Na stronie znajduje się wiele pól, z których nie wszystkie są wymagane do przeprowadzenia testu. Wartości wymagane w formularzu zależą od potrzeb i zamówienia złożonego w karcie wdrożeniowej oraz ostatecznie ustalonej konfiguracji.

4. Przygotowanie przez Partnera obsługi endpointów (w technologii REST+JSON) wystawionych w API Systemu:
    - banklist – pobranie listy dostępnych banków z informacją o obsługujących je komponentach (krok opcjonalny)
    - initiate – uruchomienie procesu weryfikacji
    - start – przekierowanie klienta do komponentu
    - result – pobranie wyniku weryfikacji
5. Przygotowanie przez Partnera adresów powrotu, tzw. „landing page", na którą należy przekierować klienta po wyjściu z systemu, gdzie powinien on oczekiwać na wynik weryfikacji.
6. Przygotowanie adresu do obsługi powiadomień o gotowym do pobrania wyniku weryfikacji. [OPCJONALNIE]
7. Przygotowanie adresu do obsługi powiadomień o zmianie w liście aktywnych banków. [OPCJONALNIE]

Integracja dla Partnera z wdrożonym „Przelewem weryfikacyjnym"

Partner może być już zintegrowany z usługą wystawianą przez BM - Przelew weryfikacyjny.

Połączenie się z ID HUBem nie wyklucza współistnienia Przelewu weryfikacyjnego jako równoległego mechanizmu weryfikacji.

Jeśli jednak Partner życzyłby sobie, aby Przelew weryfikacyjny został, zgodnie z koncepcją ID HUBa przykryty jednym interfejsem i był używany jako komponent jednej usługi, nie da się niestety dokonać migracji bezobsługowej i prace techniczne w aplikacji Partnera będą konieczne.

Konfiguracja biznesowa (sposoby realizacji zwrotów, rozliczenia prowizji itp.) jak i część konfiguracji technologicznej (rodzaje zwracanych przez przelew weryfikacyjny podsumowań, raportów, uruchamiane podsystemy) pozostaną bez zmian, przeniesione zostaną do integracji w nowym modelu.

Odmienny będzie start weryfikacji, przekierowanie klienta i sposób odebrania ostatecznego wyniku.

Środowiska

Do użytku Partnera przygotowane są dwa środowiska: testowe i produkcyjne.

> **UWAGA:** Łącząc się do Aplikacji pod podanymi wyżej adresami rekomendujemy używanie protokołu TLS w wersji przynajmniej 1.2. Obsługa wersji niższych zostanie w niedługim czasie wycofana.

Środowisko testowe

- Aplikacja: https://id-hub-accept.bm.pl/api
- API Swagger: https://id-hub-accept.bm.pl/swagger/
- Aplikacja testująca: https://id-hub-accept.bm.pl/test/start

Środowisko produkcyjne

Aplikacja: https://id-hub.bm.pl/api

Modele integracji

Partner może zintegrować się z ID HUB korzystając z następujących modeli: standardowy, standardowy z dedykowanym frontendem, White Label.

Model standardowy

1. Paywall dostępny jest po stronie Blue Media
2. Partner inicjuje weryfikację
3. Przekierowanie Klienta do frontendu Blue Media
4. Klient realizuje proces
5. Klient powraca do systemu Partnera

Model standardowy z dedykowanym frontendem

> **WSKAZÓWKA:** Opis tego modelu jest analogiczny do modelu standardowego. Różni się frontend, którego wygląd może zostać spersonalizowany przez Partnera.

1. Paywall dostępny jest po stronie Blue Media
2. Partner inicjuje weryfikację
3. Przekierowanie Klienta do spersonalizowanego frontendu
4. Klient realizuje proces
5. Klient powraca do systemu Partnera

White Label

> **WSKAZÓWKA:** Cechą modelu White Label jest większa kontrola Partnera nad działaniami Klienta oraz minimalizacja czasu przebywania Klienta poza domeną Partnera (który ogranicza się tylko do przekierowań przez strony Blue Media i pobytu w banku).

1. Paywall dostępny jest po stronie Partnera
2. Partner inicjuje weryfikację
3. Przekierowanie Klienta wprost do banku
4. Klient realizuje proces
5. Klient powraca do systemu Partnera

W tym sposobie integracji pojawia się nowa metoda API – BankList. Partner wywołuje tę metodę i w odpowiedzi otrzymuje listę skonfigurowanych dla niego dostępów bankowych.

Dostępne są dwa rodzaje dostępów: 1PLN i AIS. W ramach 1PLN mamy dodatkowo podział na dostępy: PayByLink oraz Szybki przelew. Na etapie integracji Partner ma możliwość zdania się na zespół BM w doborze banków i przypisanych do nich komponentów, ma też możliwość ustalić listę banków skrojoną pod precyzyjne zapotrzebowanie. Pobrana lista banków powinna zostać wyświetlona klientowi celem wybrania dostępnego mu kanału weryfikacji.

Na Partnera spada obowiązek odebrania od klienta stosownych zgód. Rodzaje zgód i ich treści ustalane są z zespołem BM przed rozpoczęciem prac integracyjnych.

Gdy klient wybierze bank, w którym ma rachunek, przechodzimy do inicjacji weryfikacji za pomocą metody opisanej w głównej części dokumentacji, uzupełnionej o pole z identyfikatorem banku. Partner otrzymuje adres przekierowania klienta.

Klient po dostaniu się na widok swojego banku autoryzuje systemom BM dostęp do swoich rachunków lub realizuje przelew. Uwaga, w przypadku komponentu AIS i skanowaniu historii dłuższej niż 90 dni, klient może być przekierowany do domeny BM celem wykonania dodatkowej autoryzacji SCA.

Klient jest przekierowywany z powrotem, wprost do serwisu Partnera z chwilowym „przeskokiem" przez domenę BM.

Pobranie raportu realizowane jest standardowym trybem, przy użyciu metody API - Result.

Tryby pracy ID HUB

Pobieranie danych klienta

Jest to tryb, który nie przeprowadza żadnych weryfikacji. Służy pobraniu danych Klienta z zewnętrznych źródeł. Partner ma wówczas możliwość dokonania weryfikacji danych Klienta własną metodą.

W trybie pobierania danych system przekierowuje Klienta do wybranego komponentu. Tam Klient autoryzuje dostęp Usługi do jego danych albo wprowadza je samodzielnie (Fotoweryfikacja).

HUB pobiera dane dostępne w danym komponencie i przekazuje je do Partnera w formie „surowej" lub wzbogacone o dodatkowe raporty (statystyczne, kategoryzujące rodzaje przelewów itp.).

Tryb pobierania danych dostępny jest w każdym oferowanym komponencie.

Weryfikacje

Wszystkie weryfikacje dokonywane przez system polegają na porównaniu danych deklarowanych przez Klienta, z danymi jakie otrzymamy z wybranego komponentu.

Pozyskiwane z komponentów dane klientów są skomplikowane (pod względem braku ustandaryzowanej struktury, nieprzewidywalnej kolejności elementów, różnorodności adresów, imion i nazwisk), nie gwarantujemy 100% poprawnej klasyfikacji danych, a w konsekwencji 100% poprawności wyniku porównania danych.

Żeby współczynnik skuteczności cięcia i porównywania danych mieć jak na najwyższym poziomie posługujemy się szeregiem instrumentów i algorytmów, które mają w tym pomóc.

Cięcie danych

Dane adresowe, jakie komponenty Systemu zbierają ze swoich źródeł przybierają różne formaty.

Przykłady zbieranych danych:

```
IZABELA ZIELIŃSKA Warszawska 39/14, 58-400 Kamienna Góra
KOWALSKI MARCIN ul. OSIEK 990, 63-920 OSIEK
WRÓBLEWSKI MARCIN JERZY CEYNOWY 136/15 77-100 BYTÓW
ORGANEK MARTA I ORGANEK WANDA NADWIŚLAŃSKA 82/4 03-349 WARSZAWA
GOSPODARSTWO ROLNE KAMIL MARECZEK BODZIEJOWICE 7B 42-446 IRZĄDZE
```

```
JĘDRZEJ NOREK JADWIGA JASKÓŁA-NOREK BRZEŹNICKA 1C32-700 BOCHNIA PL
NIKODEM ARLETA JANA III SOBIESKIEGO 2/6 21-500 BIAŁA PODLASKA
JANUSZ-STOLARCZYK JANINA KOSZARSKO 1 22-335 ŻÓŁKIEW KA
```

Narzędzie do cięcia danych musi w liniach takich jak powyższe (i innych) rozpoznać:

1. Imię
2. Nazwisko
3. Ulicę
4. Numer domu
5. Numer klatki schodowej
6. Numer lokalu
7. Kod pocztowy
8. Miejscowość

Nieprzewidywalny i niedeterministyczny charakter danych agregowanych z zewnętrznych źródeł wymusza na Systemie posiłkowanie się specjalnymi technikami, aby podział linii na konkretne porcje danych był jak najbliższy ideału.

Do technik tych zaliczamy:

1. Stosowanie słowników imion i nazwisk z rejestru Pesel
2. Weryfikowanie adresów przy użyciu baz adresowych i kodów pocztowych

Przyjęty sposób działania może generować nieoczekiwane rezultaty (i w efekcie nieudane procesy weryfikacyjne) dla użytkowników legitymujących się danymi adresowymi spoza obszaru Polski oraz imieniem i nazwiskiem spoza bazy Pesel (analogicznie, gdy w danej wejściowej jest nazwa firmy).

Partner może obserwować niesatysfakcjonujące wyniki działania cięcia i weryfikacji danych w sytuacji, gdy użyty komponent pobiera dane z rachunku bankowego, który jest objęty współwłasnością z inną osobą. Taki rachunek uniemożliwia jednoznaczną identyfikację klienta i użytkownika Systemu.

Porównywanie danych

W procesie weryfikacji danych klienta, krytycznym i kluczowym krokiem jest porównanie danych zadeklarowanych przez Klienta z danymi jakie uzyskaliśmy o nim w wybranym Komponencie.

Ścieżki porównywania danych

1. Ścieżka standardowych trybów

System dysponuje kilkunastoma predefiniowanymi trybami porównań. Tryby te określają jakie pola ze zbioru danych użytkownika mają być porównywane. Najpopularniejsze używane tryby to NAME_ONLY – porównujący tylko imię i nazwisko, NAME_AND_ADDRESS_ONLY – porównujący imię, nazwisko i wszystkie pola adresowe. Inne tryby powstały na potrzeby konkretnych wymagań Partnerów i są proponowane po zapoznaniu się z konkretnymi wymaganiami Partnera na etapie integracji.

W ścieżce trybów standardowych mechanizm dokonuje porównywania danych normalizując wszystkie słowa: ignoruje wielkość liter i pomija znaczenie znaków diakrytycznych.

2. Ścieżka trybów indywidualnych

W tej ścieżce partner otrzymuje możliwość indywidualnego skalibrowania sposobu porównywania pól. Lista pól branych pod uwagę przy porównywaniu jak i metodyka porównawcza może być profilowana zależnie od wymagań. Do możliwych do określenia parametrów porównywania zaliczamy:

a. Listę pól – np. imię, nazwisko, numer klatki schodowej
b. Tolerancję – determinuje czy wartości „Jan" i „Jan Piotr" w procesie porównania to wynik pozytywny, częściowo pozytywny, czy negatywny
c. Wrażliwość na wielkość znaków
d. Wrażliwość na występowanie znaków diakrytycznych
e. Procesowanie prefiksów ulic – określa czy w procesie porównania nazw ulic mamy oczyszczać pola z prefiksów typu „ul.", „płk", „abp", itp.
f. Dopuszczalną pomyłkę w słowie – określana na bazie odległości Levensteina dla słów o ustalonej minimalnej długości

W ścieżce trybów indywidualnych udostępniamy możliwość wykrywania prób popełnienia fraudów. Mechanizm testuje czy dla danego numeru rachunku usiłowano w przeszłości (od momentu włączenia tego mechanizmu) zweryfikować dane innym zestawem parametrów. Jeśli wynik sprawdzenia jest pozytywny, wszystkie kolejne weryfikacje będą automatycznie ustawiane jako negatywne.

Dane osobowe

Tryb weryfikacji danych osobowych polega na weryfikacji danych zadeklarowanych przez Klienta, danymi, które System pobiera z m.in. systemów bankowych.

Dane osobowe System weryfikuje za pomocą Komponentów: AIS, 1PLN, FOTO.

Dane, które Komponenty są w stanie zweryfikować

Dane	AIS	1PLN	FOTO
Imię	✔	✔	✔
Nazwisko	✔	✔	✔
Ulica	✔	✔	✔
Numer domu	✔	✔	✔
Numer klatki schodowej	✔	✔	✔
Numer mieszkania	✔	✔	✔
Kod pocztowy	✔	✔	✔
Miasto	✔	✔	✔
Numer rachunku	✔	✔	✖
Numer dowodu osobistego	✖	✖	✔
Miejscowość urodzenia	✖	✖	✔
Data ważności dowodu os.	✖	✖	✔
Numer PESEL	✖	✖	✔
Obywatelstwo	✖	✖	✔

Dane	AIS	1PLN	FOTO
Płeć	✖	✖	✔

Dane firmowe

Tryb weryfikacji danych firmowych polega na weryfikacji danych firmy zadeklarowanych przez Klienta, danymi, które System pobiera z systemów bankowych tudzież Głównego Urzędu Statystycznego.

Dane osobowe System weryfikuje za pomocą Komponentów: 1PLN.

Dane firmowe możliwe do zweryfikowania przez system

Rodzaj danej	1PLN
Ulica	✔
Numer domu	✔
Numer klatki schodowej	✔
Numer mieszkania	✔
Kod pocztowy	✔
Miasto	✔
Numer rachunku	✔
Nazwa firmy	✔
Numer regon	✔
NIP	✔

Komponenty weryfikujące

Komponent weryfikujący AIS

Komponent nazywany umownie "AIS" to podsystem ID HUB, który działa w oparciu o analizę historii rachunku bankowego Klienta.

Klient po wybraniu swojego banku, na liście banków w serwisie Partnera albo Blue Media (zależnie trybu integracji), jest przekierowywany na stronę logowania do swojego konta. Tam Klient dokonuje uwierzytelnienia i autoryzacji Systemu do pobrania historii transakcji. Klient powraca do serwisu, w którym zaczął proces i tam oczekuje, aż Komponent zakończy pobieranie i analizę danych.

Komponent AIS, oprócz weryfikacji danych klienta, ma możliwość generowania raportów i podsumowań.

Przykładowe typy raportów Komponentu AIS

Raport	Opis
Dane osobowe	Raport zawierający następujące dane osobowe: 1) Imię i nazwisko 2) Adres korespondencyjny 3) Adres meldunkowy
Zagregowane dane finansowe	Raport zawierający podsumowanie aktywności na rachunku Klienta w zadanym okresie.Transakcje grupowane są według następujących reguł: 1) Numer konta 2) Przychód/rozchód 3) Kategoria transakcji (podatki, zakupy, kredyty, itd.) Do komórek wyznaczonych przez powyższe reguły sumujemy kwoty przelewów. Raport wzbogacamy o informację o dacie pierwszego przelewu.
Dane surowe	Raport zawierający listę transakcji z rachunku Klienta w ustalonym formacie (np. CSV, JSON).
Dane o rachunkach	Lista rachunków bankowych ze szczegółowym opisem.

Dostęp do raportów

Możliwe jest także stworzenie raportów pod indywidualne potrzeby Partnera. W celu uruchomienia nowego rodzaju raportu należy skontaktować się z Opiekunem Biznesowym.

Raporty generowane przez komponent AIS nie są integralną częścią obiektu z wynikiem weryfikacji. Są one dostępne pod adresem URL, który zostanie do wyniku weryfikacji załączony. Przyczyną odseparowania wyniku weryfikacji od powiązanych z nim raportów jest rozmiar danych, jakie raport może wygenerować.

Dostęp do treści raportów wymaga autoryzacji metodą BasicAuth. Login i hasło zostaną dostarczone Partnerowi w formularzu wdrożeniowym lub na etapie integracji.

W **Przykład pełnego raportu generowanego przez komponent AIS** znajduje się przykładowy obiekt z wybranymi raportami.

W **Przykład drzewa kategorii do budowania zagregowanego raportu finansowego** znajduje się przykładowa lista-drzewo kategorii, które jest używane przy obliczaniu raportu finansowego. Istnieje możliwość indywidualnego zaprojektowania drzewa kategorii wedle potrzeb Partnera.

Komponent weryfikujący 1PLN (Przelew Weryfikacyjny)

Komponent 1PLN (Przelew Weryfikacyjny) to mechanizm weryfikacji Klienta, w którym użytkownik dokonuje przelewu ustalonej kwoty na rachunek bankowy Blue Media.

Po otrzymaniu przelewu, Komponent sprawdza, czy przekazane z banku informacje o nadawcy są zgodne z danymi otrzymanymi w momencie inicjacji weryfikacji. Obliczony wynik przekazywany jest Partnerowi, który podejmuje dalsze kroki w procesie biznesowym Klienta.

Personalizacja konfiguracji dostępna jest dla następujących rozszerzeń:

Rozszerzenie	Opis
Predefiniowany tytuł przelewu	Każdy przelew wykonywany przez Klienta będzie w swoim tytule zawierał ustalony opis, na przykład: „Potwierdzenie zawarcia umowy z XYZ"
Inna kwota przelewu	Domyślnie użytkownik dokonuje przelewu kwoty 1 zł. Istnieje jednak możliwość konfiguracji komponentu tak, aby użytkownik dokonywał przelewu innej, ustalonej kwoty.
Zwracanie danych otrzymanych w tytule przelewu	Do obiektu z wynikiem weryfikacji dołączona zostanie struktura z danymi zawierającymi szczegóły przelewu zrealizowanego przez Klienta: firstNameFromTransfer – imię lastNameFromTransfer – nazwisko streetFromTransfer – ulica streetHouseNumberFromTransfer – numer domu streetFlatNumberFromTransfer – numer mieszkania streetStaircaseNumberFromTransfer – numer klatki cityFromTransfer – ulica postCodeFromTransfer – kod pocztowy bankAccountNumberFromTransfer – numer rachunku unseparatedDataFromTransfer – dane przed klasyfikacją

Sposoby realizacji przelewu

Przelew weryfikacyjny wykonywany w Bramce Płatniczej Blue Media może być zrealizowany za pośrednictwem czterech sposobów.

Dostępne kanały płatności:

- **Pay By Link** - przelew realizowany jest za pośrednictwem formularza wygenerowanego w bankowości elektronicznej wybranego banku. Cały proces zamyka się w kilka, do kilkunastu minut.
- **Szybki przelew** - przelew realizowany jest podobnie w metodzie Pay By Link, z tą różnicą, że dane do przelewu użytkownik musi wprowadzić w swojej bankowości ręcznie, na podstawie przedstawionej w Bramce Płatniczej formatki.
- **PSD2-PIS** - nowy sposób dokonania płatności, podobny do metody Pay By Link, realizowany przy użyciu bankowych interfejsów PSD2.
- **Elixir** - w sytuacji, gdy powyższe kanały płatności są trwale lub przejściowo niedostępne, przelew może być zrealizowany klasyczną metodą przelewu Elixir. Czas realizacji weryfikacji w tym przypadku może zająć do dwóch dni roboczych.

Weryfikacje realizowane przez komponent 1PLN są weryfikacjami, które mogą trwać długo. Czynnikami wpływającymi na ten czas są mechanizmy bankowe dokonujące transferu pieniędzy wraz z procedurami zabezpieczającymi ten proces.

W szczególnych przypadkach czas realizacji przelewu może zająć do siedmiu dni (dotyczy tygodni z następującymi po sobie dniami świątecznymi). Z tej przyczyny czas ważności weryfikacji i oczekiwania na przelew ustawiamy standardowo na 7 dni. Ten parametr może być przyczyną nienadchodzących do systemu Partnera powiadomień o zakończonej weryfikacji nawet przez kilka dni.

Komponent weryfikujący FOTO

Komponent FOTO jest mechanizmem, w którym System pozyskuje dane osobowe klienta wprost z dokumentu tożsamości (dowodu osobistego) Klienta. Prócz pozyskania danych z dokumentu, komponent umożliwia także ocenę zgodności parametrów biometrycznych klienta przy urządzeniu, z którego korzysta, z wizerunkiem znajdującym na przedstawionym dokumencie tożsamości.

Tryby weryfikacji klienta w komponencie FOTO

Dla wszystkich trybów wyższych niż DOCUMENT, następne kroki nie zostaną wykonane, jeśli weryfikacja dokumentu tożsamości nie zakończy się powodzeniem.

Klient może zweryfikować swoją tożsamość przy pomocy jednego urządzenia mobilnego albo przy pomocy dwóch urządzeń – komputera typu desktop, w którym realizuje część procesu odpowiedzialną za zgłoszenie danych do weryfikacji i telefonu, w którym przebiega proces pozyskania i przekazania zdjęć, po czym wraca do procesu realizowanego w komputerze.

Tryb	Opis
DOCUMENT	Skanowanie dowodu tożsamości. Klient przekazuje do Systemu fotografie dwóch stron dowodu osobistego, które podlegają procesowaniu OCR, a następnie tak pozyskane dane poddawane są porównaniu ze zbiorem informacji przekazanych przez Klienta w inicjacji.
LIVENESS_PASSIVE	Jest to tryb DOCUMENT rozszerzony o krok, w którym użytkownik jest proszony o pokazanie swojej twarzy do uruchomionej kamery swojego urządzenia. Klient nie będzie proszony o wykonanie żadnych czynności, prócz umieszczenia swojego wizerunku w zaznaczonym obszarze wyświetlanego ekranu. W rezultacie, prócz rozpoznania dokumentu, nastąpi uruchomiony proces porównywania wizerunku ze zdjęcia z obrazem pobranym w trakcie sesji wideo.
LIVENESS_MOVING_HEAD	Jest to tryb LIVENESS_PASSIVE rozszerzony o poproszenie Klienta o wykonaniu ruchu głową w prawo i w lewo.
LIVENESS_DOTS	Jest to tryb LIVENESS_PASSIVE rozszerzony o poproszenie klienta o wykonanie zadań, polegających na połączeniu „nosem" wyświetlonych na ekranie kropek.

Raporty zwracane w obiekcie wynikowym dla pozytywnej weryfikacji

Raport	Opis
Dane z OCR	Raport zawiera surowe dane tekstowe pozyskane z dokumentu tożsamości: gender=M (F) fullName=JAN KOWALSKI maidenName=KOWALSKI idDocumentIssueState=POL idDocumentIssueCountry=POL idDocumentIssuingDate=2011-03-31 pesel=71072404175 fullAddreess=SYMPATYCZNA 1 m.12 80-176 GDAŃSK idDocumentExpiryDate=2021-03-31 firstName=JAN lastName=KOWALSKI idDocumentNumber=ATX195511 placeOfBirth=SŁUPSK dateOfBirth=1971-07-04 idDocumentType=IDENTITY_CARD
Zdjęcia wykonane przez Klienta	Zaszyfrowane, dostępne pod zabezpieczonym URLem archiwum ze zdjęciami jakie Klient wykonał w procesie weryfikacji.
Status procesu fotoweryfikacji	Są to trzy wskaźniki: documentStatus – określa status przetwarzania dowodu tożsamości bioStatus – określa status przetwarzania parametrów biometrycznych overallStatus – określa status całego procesu i zgodności dokumentu z parametrami biometrycznymi Możliwe wartości jakie przyjmują statusy to: VERIFIED – status pozytywny INCOMPLETE – przeprowadzona weryfikacja nie pozwoliła na jednoznaczne określenie rezultatu NOT_PERFORMED – weryfikacja w ogóle się nie odbyła SUSPICIOUS – weryfikacja została wykonana i jej wynik sugeruje potencjalną próbę oszustwa

ID HUB porównuje dane otrzymane z komponentu FOTO z danymi zadeklarowanymi przez Klienta. Dane, które mają być poddane weryfikacji, powinny znaleźć się w parametrach wejściowych (szczegóły opisuje metoda Initiate).

Metody interfejsu programistycznego

BankList

GET /api/bank/v1.1/list/{partnerUuid}

Służy do pobrania listy banków powiązanych z partnerem. Odpowiedź zawiera listę banków z informacją, jakie komponenty umożliwiają przeprowadzenie subskrybowanej usługi (weryfikacja/pobranie historii transakcji) oraz aktualny status dostępności banku wraz z datą ostatniej

zmiany statusu.

BankList – Parametry wejściowe w URL

ID	nazwa	typ	wymagany	opis
n/d	partnerUuid	uuid	tak	identyfikator Partnera

Parametry wyjściowe

ID	nazwa	typ	wymagany	opis
5	banks	map<Integer, Bank>	tak	Lista banków powiązanych z profilem Partnera. Klucze mapy są identyfikatorami banku. Opis obiektu Bank w tabeli poniżej.
25	status	Przyjmuje wartości: OK, ERROR	nie	
30	description	string	nie	dodatkowy komentarz związany z akcją - komunikat informacyjny, jeśli status=OK, komunikat błędu, jeśli status=ERROR

BankList – Obiekt Bank

ID	nazwa	typ	wymagany	opis
5	name	string	tak	Nazwa banku
10	bic	string	nie	Kod BIC/SWIFT banku
15	iconUrl	string	nie	Adres URL do ikony logotypu banku
20	additionalConsentsRequired	boolean	nie	Flaga określająca konieczność wyświetlenia dodatkowych zgód dla klienta (dla modelu white label).
25	component	string	tak	Nazwa komponentu, jaki zostanie wybrany w procesie. W szczególnych przypadkach klient zostanie przekierowany do innego komponentu. Np. w przypadku nagłej niedostępności wstępnie wybranego komponentu w trakcie realizowanego procesu.

BankList – Przykład żądania i odpowiedzi

```
Request:
GET https://id-hub-accept.bm.pl/api/bank/v1.1/list/c455(...)6d89

Response:
{
  "status": "OK",
  "description": null,
  "hash": null,
  "banks": {
```

```
    "1": {
      "name": "Mbank",
      "bic": "BREXPLPWMBK",
      "iconUrl": "https://platnosci.bm.pl/pomoc/grafika/1800.png",
      "additionalConsentsRequired": true,
      "components": "AIS"
      }
    },
    "24": {
      "name": "Test Mock Bank",
      "bic": "BMMOCKBANK",
      "iconUrl": null,
      "additionalConsentsRequired": true,
      "components": "1PLN"
    }
  }
}
```

Initiate

/api/verification/v1.0/initiate

Służy do zainicjowania procesu weryfikacji w systemie. Na podstawie odebranych parametrów wejściowych i dokonanych ustaleń projektowych system wybiera odpowiedni Komponent weryfikacyjny i przygotowuje adres do przekierowania Klienta.

Initiate – Parametry wejściowe

ID	nazwa	typ i zakres danych	wymagany	opis
1	verificationId	string (^[a-zA-Z0-9-_]{1,64}+$)	nie	identyfikator weryfikacji nadany przez Partnera
5	email	string (zakres zgodny z EmailValidator z Apache Commons ver. 1.6)	nie – dla 1PLN, FOTO; tak – dla AIS	adres email klienta
10	type	enum: PERSONAL_VERIFICATION i COMPANY_VERIFICATION i DATA_HARVEST	tak	rodzaj weryfikacji do wykonania w Systemie
15	params	map<string, string>	tak	mapa parametrów wejściowych do weryfikacji przez Komponent danego typu.Lista parametrów jest określona przez typ weryfikacji (patrz pole "type")
20	partnerUuid	uuid	tak	tekstowy identyfikator Partnera
25	bankId	integer (dozwolone wartości to klucze mapy, zwracanej metodą BankList)	nie	id wybranego banku - wymagany w modelu „White Label”

Initiate – Słownik kluczy mapy „params" dla wartości pola „type": PERSONAL_VERIFICATION

parametr	dopuszczalne wartości
firstName (imię)	^[A-Za-zĘęÓóĄąŚśŁłŻżŹźĆćŃń\s]{1,32}+$
secondName (Drugie imię)	^[A-Za-zĘęÓóĄąŚśŁłŻżŹźĆćŃń\s]{1,32}+$
thirdName (Trzecie imię)	^[A-Za-zĘęÓóĄąŚśŁłŻżŹźĆćŃń\s]{1,32}+$
lastName (Nazwisko)	^[A-Za-zĘęÓóĄąŚśŁłŻżŹźĆćŃń\s]{1,32}+$
maidenName (Nazwisko panieńskie)	^[A-Za-zĘęÓóĄąŚśŁłŻżŹźĆćŃń\s]{1,32}+$
placeOfBirth (Miejsce urodzenia)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-.()]{1,64}+$
dateOfBirth (Data urodzenia)	Data z przeszłości w formacie YYYY-MM-DD
gender (Płeć)	F, M
residenceAddressStreet (Ulica)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-.]{1,64}+$
residenceAddressHouseNumber (Numer domu)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$
residenceAddressStaircaseNumber (Numer klatki)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$
residenceAddressFlatNumber (Numer mieszkania)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$
residenceAddressPostalCode (Kod pocztowy)	^[0-9]{2}-[0-9]{3}$
residenceAddressCity (Miasto)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-.()]{1,64}+$
residenceAddressCountry (Kraj)	PL
bankAccountNumber (Numer rachunku)	^([0-9]{26})$
idDocumentType (Typ dokumentu tożsamości)	IDENTITY_CARD
idDocumentExpiryDate (Data ważności dokumentu tożsamości)	Data z przyszłości w formacie YYYY-MM-DD
idDocumentIssuingDate (Data wydania dokumentu tożsamości)	Data z przyszłości w formacie YYYY-MM-DD

Initiate – Słownik kluczy mapy „params" dla wartości pola „type": COMPANY_VERIFICATION

parametr	dopuszczalne wartości
companyName (Nazwa firmy)	^.{1,150}+$
nip (Numer NIP)	^\d{10}$
Regon (Numer REGON)	^(\d{9}|\d{14})$
companyAddressStreet (Nazwa ulicy)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-.]{1,64}+$
companyAddressHouseNumber (Numer domu)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$

parametr	dopuszczalne wartości
companyAddressStaircaseNumber (Numer klatki)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$
companyAddressFlatNumber (Numer mieszkania)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-./\]{1,10}+$
companyAddressPostalCode (Kod pocztowy)	^[0-9]{2}-[0-9]{3}$
companyAddressCity (Miasto)	^[A-Za-z0-9ĘęÓóĄąŚśŁłŻżŹźĆćŃń\s-.()]{1,64}+$
bankAccountNumber (Numer rachunku)	^([0-9]{26})$

Initiate – Słownik kluczy mapy „params" dla wartości pola „type": DATA_HARVEST

W trybie pobierania danych, nie podajemy żadnych parametrów inicjalnych.

Initiate – Parametry wyjściowe

ID	nazwa	typ	wymagany	opis
5	redirectUrl	string	tak	Adres URL, na który należy przekierować klienta
10	orderUuid	uuid	tak	Identyfikator weryfikacji nadany przez System
15	status	enum	nie	Status odpowiedzi. Przyjmuje wartości: OK i ERROR
20	description	string	nie	Dodatkowy komentarz związany z akcją. Komunikat informacyjny dla status=OK, komunikat błędu dla status=ERROR

Initiate – przykład żądania i odpowiedzi

```
Request:
{
  "partnerUuid": "cc955e86-…65d2",
  "type": "PERSONAL_VERIFICATION",
  "email": "jan@example.com",
  "params": {
    "firstName": "Jan",
    "lastName": "Niezbędny",
    "residenceAddressStreet": "Ciemna",
    "residenceAddressHouseNumber": "1",
    "residenceAddressPostalCode": "89-999",
    "residenceAddressCity": "Grodkowo",
    "bankAccountNumber": "72249000052663617643733450"
  }
}
Response:
{
  "status": "OK",
  "description": null,
  "hash": null,
  "redirectUrl": "https://id-hub-accept.bm.pl/api/verification/v1.0/start/U5F9VMY8WV",
  "orderUuid": "2ed3575a-37a6-487a-a993-b753b6e4e607"
}
```

Start

GET /api/verification/v1.0/start/<code>

Metoda służy przekierowaniu klienta do Komponentu weryfikacyjnego w celu kontynuacji procesu sprawdzenia tożsamości. Przekierowanie powinno być wykonane metodą http GET.

Jedynym parametrem metody jest unikalny identyfikator nadany przez System w metodzie initiate.

Zaimplementowanie obsługi tej metody nie jest obligatoryjne. System Partnera może całkowicie polegać na adresie, jaki pojawił się w polu „redirectUrl", odpowiedzi na żądanie inicjacji weryfikacji.

Metoda start jest metodą jednorazową. Klient tylko jeden raz może zostać przekierowany do komponentu, po czym kod ulega przeterminowaniu.

Result

/api/verification/v1.1/result

Result – Parametry wejściowe

Metoda służy pobraniu wyniku weryfikacji. Odpowiedzią jest dokument ze statusem weryfikacji, informacją o użytym Komponencie oraz odnośnikami do raportów, o ile wybrany Komponent został skonfigurowany tak, by dodatkowe informacje o kliencie obliczyć i dostarczyć.

W każdym komponencie weryfikacyjnym istnieje możliwość rezygnacji z przeprowadzenia weryfikacji. Jeżeli klient jawnie dokona takiego wyboru, lub też porzuci proces na określony w konfiguracji przedział czasu, weryfikacja w Systemie otrzymuje status ABANDONED. W takiej sytuacji odpowiedź z endpointu nie zawiera żadnych dodatkowych danych o kliencie i jego danych.

W trybie DATA_HARVEST należy inaczej interpretować pole obiektu odpowiedzi - „result". Znacząca staje się tylko wartość PENDING, która stanowi, iż wynik pobierania danych nie jest jeszcze gotowy. Gdy dane uda się pobrać, pole „result" będzie miało wartość POSITIVE i będzie oznaczać, że załączony do obiektu odpowiedzi raport jest możliwy do pobrania.

Result – Parametry wejściowe

ID	nazwa	typ	wymagany	opis
1	orderUuid	uuid	tak	Identyfikator weryfikacji
5	partnerUuid	uuid	tak	identyfikator Partnera

Result – Parametry wyjściowe

ID	nazwa	typ	wymagany	opis
5	result	enum	tak	Status weryfikacji. Dopuszczalne wartości: ABANDONED – klient porzucił i nie ukończył procesu weryfikacji; POSITIVE; NEGATIVE
7	verificationId	string	nie	Identyfikator weryfikacji nadany przez Partnera

ID	nazwa	typ	wymagany	opis
10	systemsUsed	enum	tak	Użyty Komponent. Dopuszczalne wartości: AIS; 1PLN; FOTO
15	params	map<string, string>	tak	Mapa parametrów otrzymanych w metodzie initiate, w formacie <klucz>:<status> , gdzie „klucz" zgodny jest z kluczami w mapie parametrów metody initiate, a „status" to pole słownikowe enum[POSTIVIE
20	addons	map<string, string>	nie	Mapa dodatkowych parametrów zwróconych przez komponenty weryfikacyjne. Mogą to być np. adresy do wygenerowanych raportów. Szczegółowe listy zwracanych parametrów znajdują się w paragrafach opisujących komponenty weryfikacyjne
25	status	enum	nie	Status odpowiedzi. Dopuszczalne wartości: PENDING –weryfikacja nie jest jeszcze gotowa i należy ponowić zapytanie za kilka sekund; ERROR – błąd weryfikacji. Przyczyną błędu mogło być np. utracone połączenie z bankiem Klienta
30	description	string	nie	Dodatkowy komentarz związany z akcją. Dla statusu=OK komunikat informacyjny. Dla statusu=ERROR komunikat błędu

Przykład żądania i odpowiedzi

```
Request:
{
    "partnerUuid": "cc955e86-f78f-45fd-a6c8-615ae2be65d2",
    "orderUuid": "2bc300b6-ec61-481f-a51f-114f662e9c63"
}
Response:
{
  "status": "OK",
  "description": null,
  "result": "NEGATIVE",
  "verificationId": null,
  "systemsUsed": [
    "AIS"
  ],
  "params": {
    "lastName": "NEGATIVE",
    "firstName": "NEGATIVE",
    "residenceAddressPostalCode": "NEGATIVE",
    "residenceAddressStreet": "NEGATIVE",
    "residenceAddressHouseNumber": "NEGATIVE",
    "residenceAddressFlatNumber": "NEGATIVE",
    "bankAccountNumber": "NEGATIVE",
    "residenceAddressCity": "POSITIVE",
    "residenceAddressStaircaseNumber": "NEGATIVE"
  },
  "addons": {
    "reportUrl":
"https://id-hub.accept.bm.pl/ais/report/2f9a6e5d-5ac2-4b00-a3c6-cffb9380ae9a"
```

```
    }
  }
```

Health-Check

GET /api/monitoring/health-check

Metoda jest przeznaczona do testowania dostępności sieciowej API. Odpowiedzią na żądanie powinny być słowo: OK i kod odpowiedzi http: 200. Każdy inny kod i każda inna odpowiedź oznacza wystąpienie problemów z działanie ID-HUB.

BankList-notification (PUSH)

System oferuje mechanizm powiadamiania o zmianach na liście banków. Realizuje to przez notyfikację/push na ustalony adres.

Adres, na który system powinien wysyłać powiadomienia powinien zostać dostarczony przez stronę integrującą się z HUBem.

System wysyła puste żądanie i spodziewa się pustej odpowiedzi http z kodem 204.

Domyślnie HUB wysyła jedno powiadomienie i nie próbuje ponawiać go, nawet jeśli nie otrzymał kodu odpowiedzi http 204. Ponawianie powiadomień jest opcją, którą można włączyć na życzenie Partnera.

Result-notification (PUSH)

HUB może wysyłać do systemu Partnera powiadomienie, informujące o możliwości pobrania, gotowego wyniku weryfikacji.

Aby wykorzystać tę funkcjonalność, dzięki której znika konieczność cyklicznego odpytywania o rezultat weryfikacji, Partner musi przygotować endpoint, który obsłuży żądanie http POST.

ID	nazwa	typ	wymagany	opis
1	orderUuid	uuid	tak	Identyfikator weryfikacji
5	partnerUuid	uuid	tak	Identyfikator partnera

Result-notification (PUSH) – Odpowiedź

Odpowiedzią na takie żądanie powinna być pusta odpowiedzi, z kodem http 200. Po otrzymaniu jej, System uznaje powiadomienie za dostarczone. W przeciwnym wypadku ponawia żądanie z malejącą częstotliwością, aż do momentu otrzymania oczekiwanej odpowiedzi.

> **UWAGA:** Lista pól notyfikowanych do Partnera może być zwiększana. Prosimy o uwzględnienie w implementacji możliwości płynnego pojawiania się nowych pól w obiekcie powiadomienia.

Malejąca częstotliwość oznacza ponowienia w kolejnych iteracjach, gdzie każda kolejna próba odbywa się po dłuższym odstępie czasu niż poprzednia. Odstępy są liczone zgodnie z ciągiem Fibonacciego,

zgodnie z poniższą tabelą:

Próba ponownego dostarczenia	Odstęp w minutach od poprzedniej próby
1	1
2	2
3	3
4	5
5	8
6	13
…	t = (t-1) + (t-2)

Powrót klienta z komponentu do systemu Partnera

Klient kończąc proces weryfikacji w HUBie jest przekierowywany do systemu Partnera na ustalony adres powrotu.

Są dwa adresy powrotu:

1. Adres sukcesu – klient kierowany jest po poprawnie zakończonym procesie. Uwaga – negatywną weryfikację nadal traktujemy jako poprawnie zakończony proces.
2. Adres porażki – klient kierowany jest w momencie zajścia sytuacji kryzysowej, błędu systemu. Weryfikacji nie udało się przeprowadzić.

Powrót do systemu partnera wykonywany jest na adresy dokładnie taki, jak podano w konfiguracji w karcie wdrożenia.

Wzbogacenie adresu URL o identyfikator weryfikacji

Jest możliwość wzbogacenia adresu URL o jeden z poniższych dynamicznych parametrów:

parametr	opis
orderUuid	Identyfikator weryfikacji
verificationId	Identyfikator weryfikacji nadany przez Partnera w fazie inicjacji weryfikacji

UWAGA: Do adresu powrotu dodajemy tylko jeden z powyższych parametrów, nie łączymy ich.

Potwierdzenia wykonanych weryfikacji

System oferuje funkcjonalność dostarczania potwierdzeń wykonanych weryfikacji 1PLN i AIS.

Potwierdzenie wykonanej weryfikacji jest podpisanym cyfrowo dokumentem pdf, który wysyłany jest pocztą elektroniczną pod ustalony przez Partnera adres email (adres obsługiwany przez Partnera; nie adres Klienta).

Generacja potwierdzenia AIS jest wykonywana automatycznie w czasie do 24 godzin od momentu zakończenia weryfikacji. Potwierdzenie weryfikacji 1 PLN jest generowane po złożeniu zamówienia w panelu Scribe. Zamówienie może być złożone w dowolnym momencie po przeprowadzeniu weryfikacji. Sposób korzystania z panelu i składania zamówień opisuje odrębna dokumentacja.

Rekomendacje deweloperskie

Implementując obiekty transportowe do API Systemu sugerujemy taką konfigurację narzędzia serializacji i deserializacji JSON, aby tolerowała ona pojawianie się nowych pól lub ich brak. Rozwój komponentów weryfikacyjnych może skutkować pojawianiem się nowych raportów tudzież obiektów dostarczających szczegółowych danych o kliencie. Podstawową odpowiedzią na taki rozwój wypadków jest wersjonowanie API (widoczne w adresach URL), dopuszczamy jednak (nie chcąc doprowadzić do rozdrobnienia interfejsu) możliwość drobnych modyfikacji bez wersjonowania całych ścieżek.

Bezpieczeństwo

Sieć

Bezpieczeństwo sieciowe zapewniamy Partnerom poprzez udostępnienie usługi protokołem HTTPS. Każdy endpoint lub przekierowanie będą przedstawiać się sieciowo certyfikatem wystawionym dla domeny: *.bm.pl. Prócz obsługi ruchu poprzez HTTPS, mamy domyślnie ustawione filtrowanie adresów IP dla żądań przychodzących do API Systemu.

Jeśli te dwie metody zabezpieczenia sieciowego nie są dla Partnera wystarczające, dopuszczamy możliwość stworzenia dedykowanego tunelu sieciowego, którym aplikacja Partnera będzie mogła komunikować się z usługami Systemu. Zestawienie takiego tunelu wymaga odrębnych ustaleń i procesu, ponieważ nie jest to rozwiązanie dostępne w podstawowej konfiguracji.

Istnieje także możliwość kontroli ruchu między systemami Partnera i HUBem poprzez mechanizm tzw. "dwustronnego SSL-a". W tym modelu integracji system Partnera przedstawia się podpisanym przez BlueMedia kluczem. Wdrożenie tej metody zabezpieczania, podobnie jak zestawianie tunelu, wymaga odrębnych ustaleń między Partnerem, a Blue Media.

Uwierzytelnianie

Oprócz zabezpieczeń w warstwie transportowej, System stara się zabezpieczyć komunikację także w zakresie integralności przesyłanych danych. W tym celu przygotowane została metoda weryfikacji poprawności przesyłanych komunikatów o umownej nazwie „HMAC".

Polega na wyliczeniu z ciała żądania sumy kontrolnej przy użyciu jednej z obsługiwanych funkcji:

- HmacSHA256,
- HmacSHA512

Proces liczenia sumy kontrolnej angażuje tajny, specyficzny dla każdego z Partnerów klucz, który przekazywany jest razem z pozostałymi parametrami integracyjnymi.

Partner, który w procesie integracji wybierze metodę autentykacji HMAC, zobowiązany jest załączać w każdym requeście wykonywanym metodą inną niż metoda GET, dwa nagłówki:

- Hmac-Algorithm - zawierający nazwę funkcji użytej do wygenerowania sumy kontrolnej (wartość powinna zawierać się w podanej wyżej liście obsługiwanych funkcji)
- Hmac - zawierający wyliczoną wartość sumy kontrolnej

Rekomendujemy niniejszy sposób autoryzowania żądań z następujących powodów:

1. Obiekty transportowe nie muszą być wzbogacane o pole nieniosące treści biznesowej
2. Kolejność pól w obiektach transportowych jest bez znaczenia
3. Dane zabezpieczające żądania nie są elementem treści żądania, są więc nieco trudniejsze do podsłuchania/podejrzenia

Brak lub nieprawidłowa wartość nagłówka Hmac-Algorithm skutkuje kodem odpowiedzi 400.

Brak lub nieprawidłowa wartość nagłówka Hmac skutkuje kodem 401.

Przykład sposobu liczenia sumy kontrolnej (JAVA)

```
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.util.Base64;

class Authenticator {

    public static String calculateSignature(String algorithm, String secretKey, byte[]
requestPayload) {
        Mac mac = Mac.getInstance(algorithm);
        mac.init(new SecretKeySpec(secretKey.getBytes(), algorithm));
        mac.update(requestPayload);
        byte[] signature =  mac.doFinal();

        return Base64.getEncoder().encodeToString(signature);
    }
}
```

Przykład sposobu liczenia sumy kontrolnej (PHP)

```
<?php
    $code = hash_hmac('sha256', $requestPayload, $secretKey, true);
    echo base64_encode($code);
?>
```

WSKAZÓWKA: Przykłady w innych językach programowania znajdziesz na blogu Joe Kampschmidta.

UWAGA: Implementując autoryzację metodą HMAC należy zwrócić uwagę na niewidoczne znaki nowej linii, które mogą prowadzić do różnych wyników obliczonych podpisów po stronie klienta i po stronie serwera. Najbezpieczniej jest sprawić, aby wysyłany zserializowany obiekt był pozbawiony tych znaków w ogóle.

BasicAuth

Uwierzytelnianie żądań http za pomocą mechanizmu BasicAuth stosowane jest w wybranych elementach systemu, które System chce zabezpieczyć przed przypadkowym pobraniem danych przez niepowołanych użytkowników.

W bieżącej wersji dokumentacji i systemu za pomocą metody BasicAuth zabezpieczone zostały adresy pobierania raportów w komponencie AIS.

Login i hasło potrzebne do zbudowania nagłówka „Authorization" Partner otrzymuje w momencie rozpoczęcia integracji z Systemem, w karcie wdrożeniowej.

NONE

We wstępnej fazie integracji, w środowisku testowym, mamy możliwość wyłączenia mechanizmu kontroli integralności danych. Zalecamy stosowanie tej konfiguracji tylko w środowisku testowym, w początkowej fazie integracji.

Przykład pełnego raportu generowanego przez komponent AIS

Przykład przedstawia ogólną strukturę raportu. Znajdujące się w nim wartości zostały wygenerowane losowo i zależności między nimi mogą nie być spójne.

```
/* Dane osobowe */
{
      "complete": true,
      "name": "SIWAK KRYSTIAN WŁADYSŁAW",
      "address": {
        "permanent": " PIERSNO 34 55-311 PIERSNO",
        "correspondence": "NOT_AVAILABLE"
      }
}

/* Dane finansowe */
{
  "minAccountingDate": "2020-11-09",
  "resultList": [
    {
      "period": "2021-01",
      "accountList": [
        {
          "nrb": "2016(...)00010",
          "firstTransactionDate": "2021-01-08",
          "minTransactionDate": "2021-01-08 00:00:00",
          "aggregatedData": {
            "incomes": {
              "benefits": {
                "amount": 1500.0,
                "number": 1
              },
              "loanRepayment": null,
              "currencyTransfer": null,
              "own": null,
              (...)
```

```
            "card": null
          },
          "outgoings": {
            "benefits": null,
            "loanRepayment": {
              "amount": -3152.04,
              "number": 6
            },
            "currencyTransfer": null,
            "own": {
              "amount": -58.88,
              "number": 2
            },
            (...)
            "card": {
              "amount": -533.97,
              "number": 7
            }
          }
        }
      }
    ]
  },
  {
    "period": "all",
    "accountList": [
      {
        "nrb": "2016(...)00010",
        "firstTransactionDate": "2020-11-09",
        "minTransactionDate": "2020-11-09 00:00:00",
        "aggregatedData": {
          "incomes": {
            "benefits": {
              "amount": 4938.0,
              "number": 4
            },
            "loanRepayment": null,
            "currencyTransfer": null,
            "own": null,
            (...)
            "card": null
          },
          "outgoings": {
            "benefits": null,
            "loanRepayment": {
              "amount": -9720.12,
              "number": 17
            },
            "currencyTransfer": null,
            "own": {
              "amount": -76.88,
              "number": 4
            },
            (...)
            "card": {
              "amount": -3577.06,
              "number": 44
            }
          }
        }
      }
    ]
```

```
    }
  ]
}

/* Dane o rachunkach */
{
  "accounts": [
    {
      "nrb": "1324(...)48985",
      "ownerName": "JAN NOWAK",
      "ownerAddress": "Hokejowa 18/1 80-800 Gdańsk",
      "ownerType": "INDIVIDUAL",
      "currency": "PLN",
      "accountType": "4200",
      "availableBalance": 2377.48,
      "bookingBalance": 2525.59
    }
  ]
}

/* Dane „surowe” */
[
  {
    "id": 1836180,
    "accountedAt": "2020-04-05 12:00:00",
    "operationType": "OUTGOING",
    "amount": -903.00,
    "title": "Jula Gdańsk 14/05/2020",
    "senderNrb": "42249000054378056155231380",
    "senderName": null,
    "senderAddress": null,
    "recipientNrb": "38249000051715780005877245",
    "recipientName": "52523 2418W4560C",
    "recipientAddress": "Powstańców Warszawy 6, 81-718 Sopot",
    "currency": "PLN",
    "category": "CARD"
  },
  {
    "id": 1836181,
    "accountedAt": "2020-04-27 12:00:00",
    "operationType": "INCOMING",
    "amount": 149.00,
    "title": "Żabka Sklep - SP.J.Braniewo",
    "senderNrb": "43116022020000000338556705",
    "senderName": "JĘDRZEJ ZAREMBA",
    "senderAddress": null,
    "recipientNrb": "42249000054378056155231380",
    "recipientName": "Vivus Finance",
    "recipientAddress": "Powstańców Warszawy 6, 81-718 Sopot",
    "currency": "PLN",
    "category": "UNSPECIFIED"
  },
  ...
]
```

Przykład drzewa kategorii do budowania zagregowanego

raportu finansowego


```
{
    "category": "Nieokreślone",
    "reportName": "unspecified",
    "children": [
        {
            "category": "Zablokowane transakcje",
            "reportName": "blockedTransactions",
            "children": []
        },
        {
            "category": "Przelew rodzinny",
            "reportName": "ownFamily",
            "children": []
        },
        {
            "category": "Przelew na telefon",
            "reportName": "phoneTransfer",
            "children": []
        },
        {
            "category": "Podatki",
            "reportName": "tax",
            "children": []
        },
        {
            "category": "Przelew walutowy",
            "reportName": "currencyTransfer",
            "children": []
        },
        {
            "category": "Transakcja gotókowa",
            "reportName": "cash",
            "children": []
        },
        {
            "category": "Zasiłki",
            "reportName": "benefits",
            "children": []
        },
        {
            "category": "Transakcja kartowa",
            "reportName": "card",
            "children": []
        },
        {
            "category": "Dobroczynność",
            "reportName": "charity",
            "children": []
        },
        {
            "category": "Zakupy",
            "reportName": "shopping",
            "children": []
        },
        {
            "category": "Przelew własny",
            "reportName": "own",
            "children": []
```

```
        },
        {
            "category": "ZUS",
            "reportName": "zus",
            "children": []
        },
        {
            "category": "Paliwo",
            "reportName": "petrol",
            "children": []
        },
        {
            "category": "Hazard",
            "reportName": "gambling",
            "children": []
        },
        {
            "category": "Komornik",
            "reportName": "bailiff",
            "children": []
        },
        {
            "category": "Alimenty",
            "reportName": "alimony",
            "children": []
        },
        {
            "category": "500+",
            "reportName": "plus500",
            "children": []
        },
        {
            "category": "Przelew weryfikacyjny",
            "reportName": "verification",
            "children": []
        },
        {
            "category": "Rachunki",
            "reportName": "bill",
            "children": []
        },
        {
            "category": "Spłata pożyczki",
            "reportName": "loanRepayment",
            "children": []
        },
        {
            "category": "Pożyczki",
            "reportName": "loan",
            "children": []
        },
        {
            "category": "Wypłata",
            "reportName": "salary",
            "children": []
        },
        {
            "category": "Zwroty transakcji",
            "reportName": "returnTransactions",
            "children": []
        }
    ]
```

```
}
```