# Sygnet - skalowanie procesu KYC poprzez bankowe poświadczenie tożsamości klienta

Wersja 5.1 (22/05/2018)

Proponujemy rozwiązanie w zakresie KYC, które bazując na legislacji PSD2 umożliwia wykorzystanie, będącej w posiadaniu banku, informacji o tożsamości klienta. Skalowanie procesu KYC uzyskujemy poprzez, uzyskane od banku, kryptograficzne poświadczenie tożsamości klienta. Dzięki temu bank, oprócz świadczenia usług finansowych, jest w stanie radykalnie ułatwić swoim klientom proces weryfikacji KYC w sytuacji, gdy chcą oni skorzystać z usług innych podmiotów w branży FinTech (zarówno bankowych jak i niebankowych), a w dalszej konsekwencji, staje się dla nich generatorem ich cyfrowej tożsamości w Internecie.

DISCLAIMER: Niniejszy dokument jest tylko wstępnym zarysem pomysłu i na tym etapie należy go traktować jako jedynie tekst wizjonerski. W swojej obecnej formie nie wyczerpuje on wszystkich tematów, które będą wymagać analizy, zanim ostatecznie uznamy, że opisane rozwiązanie jest warte wdrożenia.

## 1. Wprowadzenie

### **1.1 Jak weryfikować tożsamość online?**

Internetowa weryfikacja tożsamości to próba rozwiązania następującego problemu: w jaki sposób w warunkach online uzyskać pewność, że osoba (klient) podająca się jako K rzeczywiście jest tą osobą K?

Istotne jest tu to, że jest to sytuacja online, czyli nie w realu. W sytuacji kontaktu w realu dokument ze zdjęciem można uznać za wystarczająco dobry sposób weryfikacji tożsamości (mimo swoich oczywistych wad: jest kosztowny w produkcji i relatywnie łatwo może być podrobiony, zwłaszcza w przypadku, gdy nie wiemy jak dokładnie powinien wyglądać oryginalny dokument, np. dowód tożsamości obcokrajowca).

Z oczywistych powodów w warunkach online zdjęcie, które jest integralną częścią dokumentu tożsamości, przestaje być użyteczne, bo nie ma go z czym porównać.

### **1.2 Problem: nieskalowalność KYC**

Wymogi KYC narzucają na firmy konieczność ustalenia tożsamości każdego nowego klienta.

Wszystkie obecne procedury KYC mają jedną istotną wadę: nie skalują się. Przy pozyskaniu nowego klienta każda firma, która podlega wymogom KYC, musi samodzielnie dokonać ustalenia jego tożsamości, co jest kosztowne (dla firmy) i czasochłonne (dla obu stron: firmy i jej klienta). Tak więc w obecnie istniejącym paradygmacie ten sam kosztowny i czasochłonny proces musi być wykonywany wielokrotnie przez kolejne firmy.

Jedynym znanym nam sposobem na skalowanie KYC jest wykorzystanie procedury tzw. testowego przelewu, który polega na tym, że klient poświadcza swoją tożsamość poprzez wykonanie przelewu ze swojego rachunku w innym banku do banku, który potrzebuje dokonać weryfikacji KYC. Oczywiste są wady tego rozwiązania:

* nie rozwiązuje to problemu dla podmiotów niebankowych,
* nie skaluje się więcej niż raz (bo nie można w ten sposób potwierdzić tożsamości w kolejnym banku),
* wymaga to od klienta dodatkowego wysiłku.

Niemniej tego rodzaju kombinowanie (tj. używanie przelewu bankowego do celów niefinansowych) pokazuje, że problem nieskalowalności KYC rzeczywiście istnieje.

Warty podkreślenia jest fakt, że outsourcing procesu KYC do specjalistycznej firmy, która się tym zajmuje, nie rozwiązuje problemu skalowania KYC. Nawet jeśli podmiot specjalizujący się w KYC dostanie zlecenie weryfikacji klienta K, którego wcześniej weryfikował dla innej firmy, to i tak cały proces KYC będzie musiał być uruchomiony od nowa, bo nie ma żadnego formalnego dowodu, że w obu przypadkach jest to rzeczywiście ten sam klient K.

### **1.3 Co chcemy osiągnąć?**

Szukamy rozwiązania dla procesu KYC, które:

* umożliwi skalowanie procedury KYC, czyli wyeliminuje konieczność powtarzania tego procesu przez kolejne firmy,
* będzie działać dla wszystkich firm, które podlegają wymogom KYC (tj. nie tylko dla podmiotów bankowych), a także dla firm które nie są prawnie zobligowane do KYC, ale chcą to robić dla własnych potrzeb,
* będzie miało realną szansę na masową adopcję, zarówno po stronie biznesów jak i ich klientów,
* otworzy drogę na inne niż KYC zastosowania, w szczególności do rozpowszechnienia koncepcji cyfrowej tożsamości.

## 2. Skalowalny proces KYC

### **2.1 Założenia**

Najogólniej mówiąc, skalowalny KYC polega na tym, że jeden podmiot (w naszym przypadku bank) przeprowadza weryfikację tożsamości danej osoby (klienta) K, a następnie wynik tej weryfikacji jest udostępniany innym podmiotom (bankowym i niebankowym).

Do konstrukcji skalowalnego KYC wykorzystujemy następujący zestaw założeń:

* (niemal) każdy dorosły człowiek ma konto w banku,
* każdy bank zna tożsamość każdego swojego klienta,
* w ramach wprowadzonego przez PSD2 API możliwe jest wydobywanie z banku informacji dotyczących tożsamości danego klienta,
* każdy bank dysponuje [kwalifikowanym podpisem elektronicznym](https://pl.wikipedia.org/wiki/Podpis_kwalifikowany) i może go użyć do kryptograficznego podpisywania informacji przesyłanych poprzez API.

Naturalną konsekwencją wydaje się zatem istnienie możliwości zrobienia użytku z informacji o tożsamości klientów bankowych (tj. informacji, które banki i tak posiadają) w celu radykalnego usprawnienia procesu KYC.

### **2.2 System Sygnet**

W dalszej części niniejszego dokumentu opisujemy propozycję systemu o nazwie Sygnet, który realizuje koncepcję skalowania KYC przy wykorzystaniu konkluzji płynących z powyższych założeń.

Nazwa Sygnet w zamierzeniu kojarzyć się ma (zarówno w języku polskim jak i angielskim) z własnoręcznym podpisem i ma nawiązywać do czegoś, co służy do potwierdzania tożsamości użytkownika i autoryzacji różnego rodzaju działań.

Signet - a small seal, especially one set in a ring, used instead of or with a signature to give authentication to an official document.

### **2.3 Koncepcja**

System Sygnet osiąga skalowanie procesu KYC poprzez, uzyskane od banku, kryptograficzne poświadczenie tożsamości klienta. Poświadczenie to jest generowane za zgodą klienta przez jego bank i udostępniane naszemu systemowi poprzez bankowe API na mocy legislacji PSD2.

Oczywiście zakładamy tutaj, że system autoryzacji banku działa poprawnie, co oznacza, że tylko osoba która jest klientem K, może uzyskać od banku poświadczenie dotyczące tożsamości klienta K.

Patrząc z dwóch różnych perspektyw możemy powiedzieć, że:

* Z punktu widzenia użytkownika aktywnego (tj. firmy F której obowiązkiem jest przeprowadzenie procesu KYC) system Sygnet umożliwia wykorzystanie do celów KYC podpisanego elektronicznie przez bank certyfikatu poświadczającego tożsamość klienta.
* Z punktu widzenia użytkownika pasywnego (tj. klienta K który jest obiektem KYC) system Sygnet umożliwia dostarczenie dowolnej firmie podpisanego elektronicznie przez bank certyfikatu poświadczającego jego tożsamość.

Oznacza to, że nasz pomysł w zakresie KYC sprowadza się de facto do tego: w kontrolowany sposób wyprowadzamy na zewnątrz informacje (tj. dane osobowe klienta), które do tej pory leżały bezużytecznie (z perspektywy świata zewnętrznego) w systemie bankowym. Dzięki temu bank, oprócz świadczenia usług finansowych, staje się generatorem cyfrowej tożsamości swoich klientów.

### **2.4 Forma działania**

W swojej wersji podstawowej system Sygnet może być zrealizowany w formie prostej usługi webowej. W zakresie funkcjonalności interfejsu istotne jest jednak rozróżnienie między dwoma typami użytkowników:

* Dla użytkownika aktywnego (tj. firma F) potrzebny będzie bardziej rozbudowany interfejs stwarzający możliwość stworzenia konta w naszym systemie.
* Dla użytkownika pasywnego (tj. klient K) wystarczy prosty interfejs o nieograniczonym dostępie, tj. nie wymagający zakładania konta i logowania. Możliwe jest stworzenie do tego celu dedykowanej aplikacji mobilnej, ale dla potrzeb MVP prawdopodobnie nie będzie to konieczne.

### **2.5 Wymagania**

Aby system Sygnet mógł poprawnie funkcjonować potrzebne jest spełnienie następujących warunków:

1. Wymagane jest żeby nasz partner bankowy zgodził się kryptograficznie podpisywać informacje udostępniane w ramach wprowadzonego przez PSD2 API (w szczególności chodzi nam o dane osobowe klienta). Tak więc wymaganą inwestycją ze strony banku jest dostarczenie dodatkowej, tj. nie wymaganej przez PSD2, funkcjonalności w swoim API.
2. Aby system mógł być realnie użyteczny w zakresie KYC, docelowo powinno w nim uczestniczyć co najmniej kliku partnerów bankowych. Potrzebne więc będzie wystandaryzowanie procesu tak, żeby firma F otrzymywała dane KYC w jednolitym formacie niezależnie od instancji banku, który jest ich źródłem.
3. Integralną częścią naszej aplikacji musi być możliwość weryfikacji certyfikowanego podpisu elektronicznego banku, tak żeby firma F mogła w łatwy sposób uzyskać pewność, że otrzymane od banku B informacje na temat klienta K rzeczywiście zostały przez ten bank wygenerowane i nie zostały zmodyfikowane po ich podpisaniu. Jest to funkcjonalność podobna do tej, która jest oferowana przez powszechnie dostępne serwisy internetowe, np. [MadKom](https://madkom.pl/weryfikacja-podpisu-elektronicznego/).
4. Ponieważ my, jako twórcy i operatorzy aplikacji mobilnej będącej w posiadaniu klienta K, pełnimy rolę TPP (Third Party Provider), musimy być podmiotem zarejestrowanym w KNF zgodnie z wymaganiami PSD2. Wydaje się, że licencja AIS (Account Information Service) w tym przypadku będzie wystarczająca.

### **2.6 Schemat procesu**

Załóżmy, że firma F potrzebuje dokonać weryfikacji KYC klienta K i ma zaufanie do banku B, tj. podpisane elektronicznie oświadczenie banku B w zakresie tożsamości klienta K uznaje za prawdziwe.

Wtedy proces KYC w systemie Sygnet może wyglądać następująco:

1. Klient K zainteresowany skorzystaniem z usług firmy F, potwierdza, że ma konto w banku, który jest wspierany przez system Sygnet i wybiera ten system jako mechanizm weryfikacji tożsamości w procesie KYC.
2. Klient K jest przekierowany na stronę webową systemu Sygnet. Przekierowanie zawiera wygenerowany przez firmę F unikalny identyfikator ID, którego rolą jest uwiarygodnienie niniejszego procesu z punktu widzenia firmy F: uzyska ona w ten sposób pewność, że odpowiedź banku B zostanie wygenerowana specjalnie dla tej konkretnej sytuacji.
3. W ramach systemu Sygnet klient K loguje się do swojego banku B, a następnie autoryzuje wygenerowane przez system Sygnet zapytanie do bankowego API. Zapytanie to dotyczy danych osobowych klienta K, które są wymagane w procesie weryfikacji KYC, a także zawiera wyżej opisany identyfikator ID.
4. W odpowiedzi na wyżej opisane zapytanie, bank B zwraca podpisany elektronicznie pakiet zawierający i łączący w jedną całość wymagane w KYC dane osobowe klienta oraz wyżej opisany identyfikator ID.
5. Po weryfikacji podpisu banku B i identyfikatora ID firma F uznaje uzyskane od banku dane osobowe klienta K za prawdziwe i aktualne, i tym samym spełniające kryteria KYC.

### **2.7 Ochrona przed nieautoryzowanym rozpowszechnianiem**

Nasuwa się pytanie, czy firma F po uzyskaniu kryptograficznie podpisanego pakietu informacji KYC od banku B nie przekaże go kolejnej firmie, negując tym samym jej motywację do korzystania z naszego systemu.

Możliwe jest zmodyfikowanie powyższego schematu działania w taki sposób, aby zapobiec tego rodzaju nadużyciu.

Zmodyfikowany proces mógłby wyglądać następująco:

1. Oprócz unikalnego identyfikatora ID, firma F wysyła do systemu Sygnet swój klucz publiczny.
2. Zarówno identyfikator ID jak i klucz publiczny firmy F są przekazywane do banku B, który generuje pakiet KYC w sposób opisany powyżej, ale przed podpisaniem go własnym kluczem, szyfruje go kluczem publicznym firmy F.
3. Firma F po otrzymaniu pakietu jest w stanie go odkodować i zweryfikować prawdziwość zawartych w nim danych.

Tym samym przekazanie przez firmę F otrzymanego od banku pakietu KYC innej firmie przestaje mieć sens, bo wymagałoby to także ujawnienia swojego klucza prywatnego umożliwiającego jego rozkodowanie, do czego firma F nie będzie skłonna.

## 3. Kierunki potencjalnego rozwoju systemu

### **3.1 Podpis cyfrowy niewymagający klucza prywatnego**

Zauważmy, że zaprezentowany powyżej schemat systemu Sygnet można opisać w sposób następujący: klient K przekazuje do banku B dowolny ciąg znaków (np. wygenerowany przez firmę F identyfikator ID), a bank B zwraca, podpisany kryptograficznie swoim kluczem prywatnym, pakiet zawierający i łączący w jedną całość dwa elementy:

* dane osobowe klienta K, które pozwalają na jego jednoznaczną identyfikację (np. imię, nazwisko, nr dowodu osobistego albo PESEL),
* wyżej wspomniany ciąg znaków w formie nienaruszonej.

Łatwo jest zauważyć, że zamiast identyfikatora ID, który jest niczym innym niż losowym (i przez to unikalnym) ciągiem znaków, moglibyśmy użyć ciągu znaków, który jest nielosowy i przez to może być nośnikiem jakiegoś znaczenia, w szczególności być hashem dowolnego dokumentu, np. oświadczenia woli albo umowy cywilno-prawnej.

Idąc tym tropem widzimy, że system Sygnet może nie tylko służyć do skalowania procesu KYC, ale także funkcjonować jako ogólny mechanizm podpisywania przez bank w imieniu swojego klienta (i na jego żądanie) dowolnego dokumentu. (W rzeczywistości podpisywany jest hash dokumentu, a nie sam dokument, ale z punktu widzenia kryptografii efekt jest ten sam).

Oznacza to, że pod względem kryptograficznej wiarygodności uzyskujemy de facto ten sam efekt, który mielibyśmy, gdyby klient K używał swojego własnego certyfikowanego podpisu elektronicznego, a podmiotem certyfikującym ten podpis byłby jego bank.

Efekt jest ten sam, jednak z punktu widzenia user experience uzyskujemy istotny atut: w naszym podejściu nie wymagamy, aby użytkownik posiadał i dbał o klucz prywatny (co jest istotą podpisu elektronicznego), bo w naszym schemacie to **bank podpisuje się swoim kluczem prywatnym w imieniu i na żądanie klienta**.

Oczywistą konsekwencją powyższego rozwiązania jest to, że bank może uzurpować sobie tożsamość klienta (tj. podpisać się pod czymkolwiek za niego bez jego wiedzy), ale taki jest nieusuwalny trade-off tego rodzaju rozwiązania. Zdejmujemy z użytkownika obowiązek troski o klucz prywatny, ale odbywa się to kosztem konieczności zwiększonego zaufania do banku.

Możemy jednak przyjąć, że tego rodzaju trade-off ma sens, ponieważ fundamentem działalności bankowej tak czy inaczej jest zaufanie klienta.

### **3.2 Klucz prywatny certyfikowany przez bank**

Gdybyśmy jednak chcieli usunąć powyższy trade-off, system Sygnet w wersji “pro” mógłby mieć funkcjonalność pozwalającą na:

* wygenerowanie dla klienta K unikalnego klucza prywatnego i odpowiadającego mu klucza publicznego,
* uzyskanie od banku B elektronicznie podpisanego certyfikatu, który połączyłby w jedną całość tożsamość klienta K z jego kluczem publicznym.

Posiadając taki bankowy certyfikat, klient K w ramach systemu Sygnet mógłby posługiwać się swoim kluczem prywatnym w analogiczny sposób do posługiwania się certyfikowanym podpisem elektronicznym - oczywiście przy założeniu, że uznamy podmiot bankowy za wiarygodne źródło certyfikacji tego podpisu.

Założenie to oczywiście nie spełnia wymogów ustawy o kwalifikowanym podpisie elektronicznym, ale w praktyce biznesowej niewątpliwie jest to bardziej wiarygodne podejście niż np. metoda oferowana przez [DocuSign](https://www.docusign.com/).

### **3.3 Autoryzacja w PSD2**

Idąc dalej, w wyżej opisanej wersji “pro” (tzn. gdy klient ma swój własny klucz prywatny certyfikowany przez bank), możliwe staje się stworzenie niezależnego kanału autoryzacji dla transakcji bankowych, zgodnie z wymogami PSD2.

Podpisana przez klienta jego kluczem prywatnym zgoda na wykonanie konkretnego przelewu jest doskonałą alternatywą dla powszechnie stosowanej autoryzacji poprzez esemes.

Metoda ta ma też dodatkową zaletę w postaci możliwości bezpiecznego delegowania na inne osoby uprawnień w zakresie autoryzacji transakcji bankowych. Co więcej, autoryzacja poprzez klucz prywatny ma zastosowanie nie tylko w bankowości - może być stosowana wszędzie tam, gdzie użytkownik chce mieć pełną kontrolę nad swoją tożsamością (i związaną z nią reputacją), tak jak to np. zostało opisane w projekcie [Jolocom](https://jolocom.com/).

### **3.4 Weryfikacja unikalności użytkownika**

Istnieje mnóstwo biznesów (np. sieci społecznościowe), które nie podlegają wymogom KYC, ale mają następujący problem: jak skutecznie ograniczyć możliwość zakładania przez użytkowników fikcyjnych kont?

Wydaje się oczywiste, że system Sygnet mógłby być przydatny w tym zakresie i prawdopodobnie znacznie bardziej skuteczny niż tradycyjna metoda polegająca na weryfikacji dostępu do konta mailowego lub numeru telefonicznego. Unikalna tożsamość poświadczona przez bank ma niewątpliwie większą wiarygodność niż jakakolwiek inna metoda.

## 4. Alternatywne rozwiązania

### **4.1 Profil zaufany (ePUAP)**

Wedle [dokumentacji](https://www.gov.pl/cyfryzacja/profil-zaufany-ego-) Ministerstwa Cyfryzacji profil zaufany to bezpłatna metoda potwierdzania tożsamości obywatela w systemach elektronicznej administracji.

Profil zaufany działa jak odręczny podpis. Możesz dzięki niemu wysyłać przez Internet dokumenty i wnioski do różnych urzędów (np. wnieść podanie, odwołanie, skargę). Profil zaufany potwierdza tożsamość obywatela. Podpis potwierdzony profilem zaufanym, podobnie jak kwalifikowany podpis elektroniczny, skutecznie zastępuje w kontaktach z podmiotami publicznymi podpis własnoręczny.

Na pierwszy rzut oka profil zaufany wygląda na rozwiązanie bardzo podobne do naszego. Co więcej, podobnie jak w naszym podejściu jednym z podmiotów zdolnych do wygenerowania takiego profilu dla użytkownika jest serwis bankowy. Kilka banków w Polsce oferuje taką usługę.

Jest jednak istotna różnica: zastosowanie profilu zaufanego jest ograniczone do serwisów państwowych. Ograniczenie to wynika ze sposobu działania tego systemu: polega on na tym, że po założeniu profilu zaufanego użytkownik uzyskuje dostęp do wspólnego dla systemów państwowych mechanizmu logowania, lecz nie jest to równoważne z uzyskaniem uniwersalnej cyfrowej tożsamości. Tak więc profil zaufany z założenia nie może być rozszerzony na sferę niepaństwową i tym samym nie rozwiązuje problemu KYC dla firm.

Opinię tę potwierdza [poniższa interpretacja](https://www.piit.org.pl/__data/assets/pdf_file/0018/7236/Opinia_ekspertow_PIIT_identyfikacja_elektroniczna_31102017.pdf) Polskiej Izby Informatyki i Telekomunikacji:

Administracja publiczna nie umożliwia korzystania z Profilu Zaufanego przez podmioty komercyjne i nie daje żadnych gwarancji dotyczących jego wiarygodności w zakresie usług komercyjnych.

Niemniej porównanie naszego rozwiązania do profilu zaufanego wydaje się jak najbardziej uzasadnione. Można nawet powiedzieć, że nasz system oferuje biznesom rozwiązanie w zakresie KYC analogiczne do tego, jakie profil zaufany oferuje urzędom państwowym w zakresie mechanizmu weryfikacji tożsamości obywatela w warunkach online.

### **4.2 Krajowy Węzeł Identyfikacji Elektronicznej (KWIE)**

Wedle [dostępnej dokumentacji](http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2502) Krajowy Węzeł Identyfikacji Elektronicznej (KWIE) to planowany system identyfikacji elektronicznej integrujący środki identyfikacji wystawiane przez podmioty komercyjne (np. banki) dla potrzeb podmiotów świadczących online’owe usługi publiczne i niepubliczne.

KWIE umożliwiał będzie uwierzytelnienie użytkowników systemów teleinformatycznych korzystających z usług online podmiotów publicznych, z wykorzystaniem środka identyfikacji elektronicznej wydanego w krajowym systemie identyfikacji elektronicznej przyłączonym do tego węzła.

Podobnie jak w systemie Sygnet, głównym celem KWIE jest stworzenie pomostu między dawcami i biorcami informacji służącej do weryfikacji tożsamości:

KWIE został przewidziany jako rozwiązanie organizacyjno-techniczne, łączące z jednej strony platformy, na których udostępniane są usługi publiczne i niepubliczne, a z drugiej systemy identyfikacji elektronicznej, w ramach których wydawane będą środki identyfikacji elektronicznej oraz węzeł transgraniczny.

Wygląda na to, że KWIE jest rozwiązaniem typu permissioned system, bo podmioty uczestniczące po obu stronach (czyli dawcy i biorcy informacji) muszą spełnić dość ostre kryteria opisane w ustawie. Powody wysokich wymagań dla dawców są dość jasne: trzeba mieć pewność, że dostarczana przez nich identyfikacja tożsamości jest wiarygodna. Jednak wymogi po stronie biorców są równie wysokie, jednak ich zasadność jest dużo mniej oczywista:

System, w którym udostępniane są publiczne lub niepubliczne usługi online będzie mógł być przyłączony do węzła krajowego po zapewnieniu przez podmiot odpowiedzialny za ten system opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, po przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tych systemów z węzłem krajowym, oraz po złożeniu przez podmiot wnioskujący oświadczenia, że będzie on działał zgodnie z przepisami o ochronie danych osobowych. Minister właściwy do spraw informatyzacji przed wydaniem decyzji o przyłączeniu tych systemów może sprawdzać spełnianie wyżej wspomnianych wymagań. W przypadku niespełniania wyżej wspomnianych wymagań wydaje decyzję o odmowie przyłączenia do węzła krajowego systemu, w którym udostępniane są usługi online, nie zostanie udzielona.

Niejasny jest też model ekonomiczny systemu. Z jednej strony system [jest prezentowany](https://www.piit.org.pl/__data/assets/pdf_file/0018/7236/Opinia_ekspertow_PIIT_identyfikacja_elektroniczna_31102017.pdf) jako całkowicie bezpłatny:

Wszystkie podmioty świadczące usługę identyfikacji będą ją udostępniały na rzecz administracji publicznej bezpłatnie i nie będą pobierały opłaty za korzystanie z identyfikacji przez obywateli w usługach publicznych.

Jednak z drugiej strony nie jest jasne, jaka jest przewidywana motywacja dla dawcy tożsamości do uczestniczenia w systemie (i tym samym poddania się rygorowi ostrych kryteriów) oraz jaki jest planowany mechanizm rozliczeń między komercyjnymi biorcami i dawcami, mimo [przewidywań](https://www.piit.org.pl/__data/assets/pdf_file/0018/7236/Opinia_ekspertow_PIIT_identyfikacja_elektroniczna_31102017.pdf), że takie przepływy finansowe będą miały miejsce:

Opłaty za usługi komercyjnej identyfikacji będą ponosiły podmioty komercyjne wykorzystujące ją w swoich usługach.

Podsumowując, KWIE [jest prezentowany](https://www.piit.org.pl/__data/assets/pdf_file/0018/7236/Opinia_ekspertow_PIIT_identyfikacja_elektroniczna_31102017.pdf) jako dość jednostronne zaspokojenie potrzeb administracji publicznej bez klarownie zdefiniowanych korzyści dla sektora komercyjnego:

W ramach funkcjonowania krajowego systemu identyfikacji elektronicznej dostawcy tożsamości nie uzyskują danych z systemów administracji publicznej, tylko administracja publiczna korzysta z danych będących w posiadaniu komercyjnych dostawców tożsamości.

W tym świetle szansą Sygnetu jest dostarczenie systemu, który:

* specjalizuje się w zaspokojeniu potrzeb podmiotów komercyjnych (w odróżnieniu od potrzeb administracji publicznej, do czego będzie zapewne grawitował KWIE),
* jest znacznie bardziej zrównoważony w zakresie zapewnienia obopólnych korzyści zarówno dla dawców jak i biorców informacji.

## 5. Uzasadnienie przydatności systemu

System Sygnet ma szansę być postrzeganym jako sytuacja typu win-win dla wszystkich interesowanych, ponieważ:

1. Dostarczamy bankom możliwość monetyzowania informacji o tożsamości ich klientów, z wykorzystaniem mechanizmów autoryzacji, które zgodnie z PSD2 muszą zostać dostarczone na potrzeby TPP. Dodatkową korzyścią dla banków jest możliwość dostarczenia nowego typu usługi dla swoich klientów: oprócz oferowania im usług stricte finansowych bank może stać się generatorem ich cyfrowej tożsamości w Internecie.
2. Dostarczamy wszystkim podmiotom, których biznes podlega wymogom KYC, mechanizm szybkiej weryfikacji tożsamości klientów. Jego użycie przede wszystkim radyklanie zredukuje problemy związane z procesem KYC, a także istotnie skróci czas, jaki upływa od momentu zainteresowania klienta ofertą do momentu faktycznej sprzedaży towaru lub usługi, eliminując tym samym okazję do rozmyślenia się przed zakupem.
3. Konsument nie jest rozpraszany formalnymi wymogami i może skoncentrować się na tym, co dla niego ważne, czyli na konsumpcji. Więc także i on powinien postrzegać system Sygnet jako wyraźne udogodnienie.

System Sygnet występuje więc w roli pośrednika pomiędzy:

* biorcą informacji, czyli firmą F która potrzebuje zweryfikować nowego klienta pod kątem KYC,
* dawcą informacji, czyli bankiem B który uprzednio dokonał weryfikacji KYC dla danego klienta.

Czy ta rola pośrednika jest w naszym przypadku dobrze uzasadniona? Wydaje się że tak, bo dzięki systemowi Sygnet biorca informacji (tj. firma F) unika dwóch relatywnie trudno wykonalnych kwestii:

* nie musi posiadać statusu TPP (Third Party Provider) w PSD2,
* nie musi integrować się z wieloma bankami.

## 6. Współpraca z podmiotami niebankowymi

Wyżej opisany mechanizm weryfikacji tożsamości jest na tyle abstrakcyjny, że podmiotem będącym dawcą informacji może być nie tylko bank lecz także dowolny inny podmiot, który posiada:

* wiarygodne informacje o tożsamości swoich klientów,
* publiczne API,
* sprawnie działający system logowania dla swoich klientów.

Bank, jako dawca informacji, jest dla nas najcenniejszym partnerem, bo spośród podmiotów gospodarczych tożsamość potwierdzona przez bank jest najbardziej wiarygodna. Jednak być może optymalną strategią jest zacząć od współpracy z podmiotem niebankowym, np. Allegro, z następujących powodów:

* proces współpracy technologicznej będzie tu prawdopodobnie łatwiejszy,
* do takiego podmiotu bardziej przemawiają argumenty finansowe.

Ponadto fakt udanej współpracy z podmiotem niebankowym stawia nas w dużo lepszej pozycji negocjacyjnej podczas rozmowy z bankiem.