KNF
KOMISJA NADZORU FINANSOWEGO

Kamil Leżoń

OTWARTA BANKOWOŚĆ W ŚWIETLE WYMOGÓW DYREKTYWY PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech

KNF | KOMISJA NADZORU FINANSOWEGO

Kamil Leżoń

OTWARTA BANKOWOŚĆ W ŚWIETLE WYMOGÓW DYREKTYWY PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech

Warszawa 2019

Publikacja została wydana nakładem Urzędu Komisji Nadzoru Finansowego

© Urząd Komisji Nadzoru Finansowego
ul. Piękna 20
00-549 Warszawa
www.knf.gov.pl

Warszawa 2019
Wydanie I

ISBN 978-83-66322-03-5
Nakład: 2000 szt.
Stan prawny na dzień: 30 listopada 2019 r.

Przygotowanie do druku i druk:
Pracownia C&C Sp. z o.o.

Niniejsza publikacja wydana została w celach edukacyjnych w ramach projektu CEDUR. Informacje w niej zawarte mają wyłącznie charakter ogólny i nie stanowią porady prawnej oraz inwestycyjnej.

Urząd Komisji Nadzoru Finansowego nie ponosi odpowiedzialności za wszelkie decyzje podjęte przez czytelnika na rynku finansowym, na podstawie zawartych w niniejszej publikacji informacji.

SPIS TREŚCI

WSTĘP

Sposób korzystania z usług bankowych podlega ciągłym zmianom wynikającym przede wszystkim z dynamicznego rozwoju sektora innowacji finansowych (FinTech), ale również nowych regulacji prawnych i wzrastających potrzeb klientów, którzy oczekują odpowiedniej jakości i dostępności usług finansowych w wygodnym dla nich miejscu i czasie. Znaczące przeobrażenia można zauważyć w formie komunikacji klienta z bankiem, gdzie tradycyjna wizyta w oddziale banku w wielu przypadkach może zostać zastąpiona kontaktem wirtualnym, w szczególności z wykorzystaniem urządzeń mobilnych, m.in. smartfonów.

Kluczowym bodźcem dla rozwoju nowych rozwiązań na bazie tradycyjnych usług bankowych jest druga dyrektywa o usługach płatniczych zwana PSD2 (ang. *Payment Services Directive 2*). Spowodowała ona zmianę dotychczasowej działalności dostawców usług płatniczych, w tym banków, w kierunku modelu otwartej bankowości (ang. *open banking*) z wykorzystaniem interfejsów dostępowych API (ang. *Application Programming Interface*).

W ciągu ostatnich kilku lat nastąpiły istotne zmiany w obszarze płatności detalicznych pod względem innowacji technologicznych. Doprowadziło to do wzrostu płatności elektronicznych (w szczególności w obszarze bankowości mobilnej) oraz pojawienia się na rynku nowych rodzajów usług płatniczych, tzw. usług dostępu do rachunku (ang. *Access to Account* – XS2A). Do tej pory zasadniczo tylko klienci banków mieli bezpośredni dostęp do swoich rachunków płatniczych i możliwość zlecania transakcji płatniczych. Zgodnie z dyrektywą PSD2 filozofia dostępu do rachunków płatniczych zmieniła się znacząco, ponieważ uprawnione podmioty trzecie (ang. *Third Party Providers* – TPP) mogą w imieniu klienta uzyskać dostęp do informacji o jego rachunku lub zlecać realizację płatności.

Dyrektywa PSD2 reguluje 3 nowe rodzaje usług oferowanych przez TPP: usługę inicjowania płatności, usługę dostępu do informacji o rachunku oraz usługę potwierdzenia dostępności środków na rachunku.

Podstawowym aktem wykonawczym dyrektywy PSD2 normującym funkcjonowanie otwartej bankowości są regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klienta oraz wspólnych i bezpiecznych otwartych standardów komunikacji (ang. *Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication* – dalej: RTS).

Zgodnie z RTS każdy dostawca usług płatniczych prowadzący rachunek dostępny online (ang. *Account Servicing Payment Service Provider* – ASPSP, np. bank) zobowiązany jest zapewnić co najmniej jeden interfejs komunikacji z TPP. Ustanowiony interfejs komunikacji powinien pozwalać TPP na wzajemną identyfikację z ASPSP oraz wykorzystywanie procedur uwierzytelniania zapewnianych przez ASPSP użytkownikom

usług płatniczych. Dostawcy prowadzący rachunek mogą udostępnić interfejs komunikacji z TPP poprzez utworzenie specjalnego interfejsu API lub modyfikację oferowanego serwisu bankowości internetowej. Wybór rodzaju interfejsu należy do decyzji biznesowej ASPSP, niemniej jednak z punktu widzenia zapewnienia efektywnej kontroli nad zakresem udostępnianych danych, w opinii Komisji Nadzoru Finansowego, bezpieczniejszym rozwiązaniem jest stworzenie specjalnego interfejsu API.

Celem niniejszej publikacji jest wyjaśnienie zagadnienia otwartej bankowości, wskazanie najważniejszych wymogów regulacyjnych i prawnych wynikających z dyrektywy PSD2, RTS i ustawy o usługach płatniczych, których stosowanie może stanowić wyzwanie dla uczestników rynku, oraz przedstawienie potencjalnych perspektyw rozwoju otwartej bankowości w polskim sektorze FinTech.

Niniejsza publikacja adresowana jest do głównych interesariuszy rynku płatności, przede wszystkich dostawców prowadzących rachunki płatnicze (ASPSP), podmiotów świadczących usługi dostępu do rachunku (TPP) oraz innych podmiotów, które widzą swoją rolę w otwartej bankowości (np. firm technologicznych). Informacje zawarte w publikacji mogą być również przydatne bardziej zaawansowanym klientom usług finansowych, którzy chcieliby pozyskać wiedzę nt. otwartej bankowości.

SŁOWNIK
POJĘĆ I SKRÓTÓW

AIS (ang. *Account Information Service*) – usługa dostępu do informacji o rachunku.

AISP (ang. *Account Information Service Provider*) – dostawca świadczący usługę dostępu do informacji o rachunku. W publikacji określany również jako dostawca AIS.

ASPSP (ang. *Account Servicing Payment Service Provider*) – dostawca usług płatniczych prowadzący rachunek użytkownika (np. bank, spółdzielcza kasa oszczędnościowo-kredytowa).

API (ang. *Application Programming Interface*) – interfejs programistyczny aplikacji, rozumiany jako zestaw reguł, protokołów i narzędzi, za pomocą których programy komputerowe (aplikacje) komunikują się pomiędzy sobą. W publikacji określany również specjalnym interfejsem komunikacji z TPP.

Autoryzacja (ang. *authorization*) – w obszarze usług płatniczych oznacza zgodę użytkownika (posiadacza rachunku) na wykonanie określonej operacji w bankowości elektronicznej. Autoryzacja stosowana jest w ramach procedury SCA (ang. *Strong Customer Authentication*) po pomyślnym uwierzytelnieniu użytkownika, przyjmując formę np. wpisania kodu SMS w aplikacji mobilnej banku w celu zatwierdzenia transakcji płatniczej lub uzyskania dostępu do rachunku użytkownika. W informatyce autoryzacja odnosi się do procesu weryfikacji uprawnień podmiotu/użytkownika do korzystania z żądanego zasobu lub wykonania określonej czynności.

BigTech – sektor największych globalnych firm technologicznych działających na masową skalę w Internecie, których rozwój zmierza w kierunku świadczenia usług finansowych lub rozwiązań zbliżonych do usług finansowych. Do sektora BigTech zalicza się w szczególności amerykańskie firmy występujące pod akronimem GAFA (Google, Amazon, Facebook, Apple) oraz chińskie korporacje określane skrótem BAT (Baidu, Alibaba, Tencent).

CAF (ang. *Confirmation of the Availability of Funds*) – usługa potwierdzania dostępności środków na rachunku.

CBPII (ang. *Card-Based Payment Instrument Issuer)* – wydawca instrumentu płatniczego opartego na karcie, świadczący usługę potwierdzania dostępności środków na rachunku. W publikacji określany również jako dostawca CAF.

Certyfikat eIDAS – w publikacji rozumiany w kontekście wymogów RTS jako kwalifikowany certyfikat pieczęci elektronicznej (ang. *Qualified Certificate for Electronic Seal* – QSealC) lub kwalifikowany certyfikat uwierzytelniania witryny internetowej (ang. *Qualified Certificate for Website Authentication* – QWAC).

Dostawca usług płatniczych (ang. *Payment Service Provider* – PSP) – podmiot prowadzący działalność regulowaną w zakresie świadczenia usług płatniczych (np. bank, instytucja płatnicza, instytucja pieniądza elektronicznego, dostawca świadczący wyłącznie usługę dostępu do informacji o rachunku).

EBA (ang. *European Banking Authority*) – Europejski Urząd Nadzoru Bankowego.

ECB (ang. *European Central Bank*) – Europejski Bank Centralny.

eIDAS (ang. *Electronic Identification and Trust Services*) – usługi zaufania oraz identyfikacji elektronicznej.

EPC (ang. *European Payments Council*) – Europejska Rada ds. Płatności.

FinTech (ang. *Financial Technology*) – obszar innowacji w usługach finansowych opartych na technologiach, które mogą prowadzić do powstania nowych modeli biznesowych, zastosowań, procesów i produktów oraz mogą mieć w związku z tym znaczący wpływ na rynki i instytucje finansowe oraz na sposób świadczenia usług finansowych[1].

Fintechy – potoczna nazwa podmiotów z sektora FinTech, do których zalicza się zarówno innowacyjne firmy (często start-upy) podejmujące działalność regulowaną (lub częściowo regulowaną) na rynku finansowym, jak również innowacyjne podmioty nadzorowane (np. banki, instytucje płatnicze) wdrażające nowoczesne rozwiązania technologiczne w zakresie oferowanych produktów lub usług finansowych. W publikacji fintechy określane są również jako TPP w kontekście dyrektywy PSD2.

GAFA (skrót od: Google, Amazon, Facebook, Apple) – cztery największe amerykańskie firmy technologiczne działające na masową skalę w Internecie, których rozwój zmierza w kierunku świadczenia usług finansowych lub rozwiązań zbliżonych do usług finansowych. Firmy GAFA zaliczane są do sektora BigTech, podobnie jak duże chińskie korporacje występujące pod akronimem BAT (Baidu, Alibaba, Tencent). W niektórych opracowaniach stosuje się również rozszerzony akronim GAFAA, który, oprócz amerykańskich gigantów technologicznych, uwzględnia firmę Alibaba.

KIP – krajowa instytucja płatnicza.

KNF/UKNF – Komisja Nadzoru Finansowego/Urząd Komisji Nadzoru Finansowego.

Kod autoryzacyjny (ang. *authorization code*) – kod służący do potwierdzenia przez użytkownika zgody na realizację transakcji płatniczej lub wykonanie innej czynności w ramach bankowości elektronicznej. W specyfikacji standardu PolishAPI określany

[1] Na podstawie definicji FinTech stosowanej przez Radę Stabilności Finansowej (ang. *Financial Stability Board* – FSB): https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/

jako kod zawierający informacje o poprawnym uwierzytelnieniu użytkownika i wyrażeniu przez niego zgody na dostęp TPP do określonych usług i zasobów ASPSP.

Kod CVV/CVC (ang. *Card Verification Value/Code*) – wartość lub kod weryfikacyjny karty płatniczej (debetowej lub kredytowej) występujący zazwyczaj na jej odwrocie w postaci 3-cyfrowej, który jest wykorzystywany do autoryzacji transakcji płatniczych w Internecie.

Kod uwierzytelniający (ang. *authentication code*) – specjalny kod wygenerowany po przeprowadzeniu procedury SCA w oparciu o zastosowanie co najmniej dwóch elementów należących do różnych, spośród 3, kategorii: wiedza, posiadanie lub cecha klienta.

Opcja fallback (ang. *fallback mechanism*) – mechanizm rezerwowy określony w RTS jako środek awaryjny ASPSP na wypadek nieplanowanej niedostępności lub awarii specjalnego interfejsu komunikacji z TPP. W ramach opcji *fallback* ASPSP jest zobowiązany zapewnić zidentyfikowanym wcześniej TPP możliwość korzystania z interfejsu tradycyjnego udostępnionego użytkownikom usług płatniczych do momentu przywrócenia poziomu dostępności i efektywności specjalnego interfejsu do poziomu utrzymywanego dla interfejsu tradycyjnego.

Otwarta bankowość (ang. *open banking*) – ogół usług i technologii w obszarze finansów, opartych na otwartych interfejsach programistycznych (*Open API*), które umożliwiają stronom trzecim budowę innowacyjnych aplikacji i serwisów wykorzystujących dane lub usługi udostępnianie przez instytucje finansowe (w tym przede wszystkim banki).

Pay-by-link (PBL) – przelew bezpośredni uruchamiany specjalnie wygenerowanym linkiem. Wszystkie dane potrzebne do wykonania przelewu są wypełniane automatycznie, a klient musi tylko zatwierdzić przelew w systemie bankowości internetowej.

Phishing – metoda oszustwa polegająca na podszywaniu się pod godną zaufania instytucję (np. bank) w celu wyłudzenia informacji wrażliwych (np. login i hasło do bankowości internetowej, kod autoryzacyjny, dane karty kredytowej) albo nakłonienia ofiary do określonych działań.

PIS (ang. *Payment Initiation Service*) – usługa inicjowania płatności.

PISP (ang. *Payment Initiation Service Provider*) – dostawca świadczący usługę inicjowania płatności. W publikacji określany również jako dostawca PIS.

Płatnik – osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędącą osobą prawną, która posiada zdolność prawną, składająca zlecenie płatnicze.

PolishAPI – standard opracowany pod auspicjami Związku Banków Polskich (ZBP), we współpracy z uczestnikami rynku, który definiuje interfejs API na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych użytkowników. Istotny element otwartej bankowości na rynku polskim.

PSD (ang. *Payment Services Directive*) – Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE.

PSD2 (ang. *Payment Services Directive 2)* – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

Rachunek płatniczy – rachunek prowadzony dla jednego lub większej liczby użytkowników służący do wykonywania transakcji płatniczych, do którego użytkownik posiada dostęp w trybie online.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (ang. *General Data Protection Regulation* – GDPR).

RTS (ang. *Regulatory Technical Standard*s) – Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji.

Sandbox – informatyczne środowisko testowe zwane potocznie piaskownicą.

Specjalny interfejs komunikacji (ang. *dedicated interface*) – wdrożony przez ASPSP dedykowany interfejs komunikacji z TPP na potrzeby świadczenia usług dostępu do rachunku, zwany potocznie API. Interfejs ten powinien charakteryzować się takim samym poziomem dostępności i efektywności – w tym wsparcia – co tradycyjny interfejs użytkownika.

SCA (ang. *Strong Customer Authentication*) – silne uwierzytelnianie klienta (użytkownika) zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do różnych, spośród 3, kategorii: wiedza, posiadanie lub cecha klienta, będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych.

Screen scraping (ang. dosł. „zeskrobywanie z ekranu") – technika, za pomocą której program komputerowy automatycznie pozyskuje dane z wyjścia innego programu prezentowanego w postaci wizualnej (bez możliwości odczytu maszynowego), np. serwisu bankowości internetowej lub aplikacji mobilnej banku. W obszarze usług

finansowych *screen scraping* polega na dostępie nieznanych dla ASPSP podmiotów trzecich do rachunków płatniczych użytkowników, na podstawie udzielonej przez nich zgody i przekazanych danych uwierzytelniających do konta bankowości elektronicznej. Powyższa metoda jest niedopuszczalna w świetle wymogów RTS.

Start-up – młode innowacyjne przedsiębiorstwo poszukujące rentownego modelu biznesowego, najczęściej opartego na nowoczesnych technologiach informacyjnych. Popularnym narzędziem wspierania rozwoju start-upów są programy akceleracyjne. W publikacji start-up podejmujący innowacyjną działalność w obszarze usług finansowych określany jest fintechem.

TPP (ang. *Third Party Provider*) – podmiot trzeci świadczący nowe usługi dostępu do rachunku wynikające z dyrektywy PSD2, tj. PIS, AIS i CAF. W publikacji TPP określany jest również fintechem.

Tradycyjny interfejs komunikacji – interfejs użytkownika usług płatniczych udostępniany przez ASPSP w ramach serwisu bankowości internetowej lub aplikacji mobilnej.

Usługi dostępu do rachunku – nowe usługi wynikające z dyrektywy PSD2, tj. usługa inicjacji płatności (PIS), usługa dostępu do informacji o rachunku (AIS) oraz usługa potwierdzania środków na rachunku (CAF).

UUP – Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2019 r. poz. 659 t.j. z późn. zm.).

Uwierzytelnianie (ang. *authentication*) – procedura weryfikacji tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika (np. hasła do systemu bankowości internetowej).

UX (ang. *User Experience*) – doświadczenie użytkownika podczas korzystania z danego produktu lub usługi.

Użytkownik usług płatniczych (ang. *Payment Service User* – PSU) – osoba fizyczna lub prawna korzystająca z usług płatniczych w charakterze płatnika lub odbiorcy; użytkownikiem jest również osoba korzystająca z usługi dostępu do informacji o rachunku (AIS). W publikacji pojęcie użytkownik może być stosowane zamiennie z pojęciem klient lub konsument.

Wytyczne EBA – Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji).

XS2A (ang. *Access to Account*) – dostęp do rachunków płatniczych, wykorzystywany do wykonywania usług AIS, PIS, CAF oraz innych usług realizowanych w ramach standardu PolishAPI.

1 WPROWADZENIE DO POJĘCIA OTWARTEJ BANKOWOŚCI

Otwarta bankowość to termin, który w Polsce stał się popularny za sprawą dyrektywy PSD2 zaimplementowanej do krajowego porządku prawnego w 2018 r., ale na świecie był już stosowany kilka lat wcześniej, w szczególności w Wielkiej Brytanii[2], uważanej za prekursora rozwoju modeli działalności banków opartych na udostępnianiu danych transakcyjnych klientów podmiotom trzecim[3].

Wyjaśnienie zagadnienia otwartej bankowości należy rozpocząć od zrozumienia pojęcia API, które można zdefiniować w sposób następujący:

> **API** *(ang. Application Programming Interface)* to interfejs programistyczny aplikacji rozumiany jako zestaw reguł, protokołów i narzędzi, za pomocą których programy komputerowe (aplikacje) komunikują się pomiędzy sobą[4].

W praktyce API umożliwia komunikację pomiędzy wieloma aplikacjami, w ramach której jedna aplikacja odwołuje się do funkcjonalności innej aplikacji, np. w zakresie udostępnianych danych.

W bankowości zwykle można wyróżnić 3 podstawowe rodzaje API[5]:

1) **Wewnętrzne/prywatne API** (ang. *internal/private API*): są to interfejsy używane w ramach tradycyjnej działalności bankowej, które zwiększają wydajność operacyjną realizowanych procesów biznesowych.

2) **Partnerskie API** (ang. *partner/B2B API*): są to interfejsy umożliwiające interakcje między bankiem a określonymi partnerami zewnętrznymi, które pozwalają na rozbudowę linii produktów, usług, kanałów dystrybucji itd.

3) **Otwarte/publiczne API** (ang. *open API*): są to interfejsy, za pośrednictwem których dane biznesowe są udostępniane podmiotom trzecim, w wielu przypadkach bez ustanowienia formalnych relacji z bankiem. Specyfikacja tego rodzaju API jest dostępna publicznie. Otwarte API wykorzystywane są przez zewnętrznych developerów, którzy na bazie nowych technologii i danych klientów budują innowacyjne rozwiązania.

---

[2] Na podstawie raportu *Open Banking: Preparing for Lift Off*, wydanego przez OBIE (*The Open Banking Implementation Entity*) w 2019 r.: https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf

[3] Do krajów pozaeuropejskich rozwijających koncepcję otwartej bankowości zalicza się m.in.: Singapur, Australię, Kanadę, Indie, Stany Zjednoczone, Hong Kong, Nową Zelandię, Nigerię, Meksyk i Japonię (ibidem).

[4] http://www.webabc.pl/technologia/api, dostęp z dnia 15.11.2019 r.

[5] https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking, dostęp z dnia 15.11.2019 r.

Dotychczas banki najczęściej korzystały z API prywatnych lub partnerskich. Z biegiem czasu interfejsy API zaczęły jednak ewoluować w kierunku bardziej rozbudowanych otwartych modeli (*Open API*), co doprowadziło do pojawienia się pojęcia **otwartej bankowości** zdefiniowanej poniżej[6].

> **Otwarta bankowość** (ang. *open banking*) oznacza ogół usług i technologii w obszarze finansów, opartych na otwartych interfejsach programistycznych (*Open API*), które umożliwiają stronom trzecim budowę innowacyjnych aplikacji i serwisów wykorzystujących dane lub usługi udostępniane przez instytucje finansowe (w tym przede wszystkim banki)[7].

Pojęcie otwartej bankowości można rozpatrywać pod wieloma względami, ale najczęściej zawiera w sobie przynajmniej trzy warstwy znaczeniowe[8]:

1) **Warstwę technologiczną** – użycie określonych technologii w oparciu o otwartą architekturę interfejsów programistycznych (API).

2) **Warstwę prawną i regulacyjną** – zastosowanie określonych przepisów prawnych w kontekście udostępniania danych, realizacji usług bankowych, nadzoru nad instytucjami świadczącymi takie usług itp.

3) **Warstwę biznesową** – świadczenie usług płatniczych oraz innych usług opartych na dostępie do danych finansowych, tworzenie nowych modeli biznesowych.

Jednocześnie należy wskazać, że otwarta bankowość wpisuje się w ogólnoświatowy trend gospodarki API (ang. *API economy*), rozumianej jako model współdziałania firm, organizacji i instytucji publicznych, w którym wybierają one z zestawu publicznych i prywatnych API funkcjonalności, które mogą łatwo zintegrować, oferując w ten sposób nowe usługi dla klientów.

Interfejsy *Open API* będące podstawą funkcjonowania otwartej bankowości są od wielu lat udostępniane przez firmy technologiczne, takie jakie Google, Facebook czy Amazon. Dzięki wykorzystaniu ich inne podmioty gospodarcze są w stanie proponować swoim klientom wiele nowych usług, których same nie byłyby w stanie stworzyć[9].

Zasadę działania *Open API* można wyjaśnić na przykładzie aplikacji Uber. Otóż Google udostępnia przez swoje API interfejs map Google, a Uber z niego korzysta do oferowania własnych usług transportowych. Podobnie jest w przypadku otwartej bankowości

---

[6] Pojęcie otwartej bankowości może być zdefiniowane w różny sposób. Definicja zaproponowana w niniejszej publikacji jest jedną z przykładowych definicji stosowanych na rynku finansowym.

[7] https://pl.wikipedia.org/wiki/Otwarta_bankowo%C5%9B%C4%87, dostęp z dnia 15.11.2019 r.

[8] Ibidem.

[9] Wg raportu KPMG i Związku Banków Polskich pt. „*PSD2 i Open Banking. Rewolucja czy ewolucja?*", Marzec 2019: https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/03/pl-raport-kpmg0-zbp-psd2-i-open-banking-rewolucja-czy-ewolucja.pdf

– banki udostępniają część swoich danych czy usług, na bazie których podmioty trzecie (TPP) mają możliwość budowania nowych usług i produktów.

Dzięki współpracy i korzystaniu z *Open API*, banki i TPP mogą wykorzystywać swoje mocne strony, polepszając doświadczenia klientów (ang. *user experience* – UX) o wiele bardziej niż każdy z tych podmiotów samodzielnie.

Otwarta bankowość daje bankom możliwość utrzymania, a nawet powiększenia bazy klientów poprzez dostarczenie im różnorodnych rozwiązań, mających na celu dostosowanie produktów i usług do ich indywidualnych potrzeb. W przypadku banków, które w swojej strategii działalności nie uwzględniły koncepcji otwartej bankowości, istnieje duże prawdopodobieństwo, że mogą stracić lub znacznie osłabić dotychczasowe bezpośrednie relacje ze swoimi klientami.

2 REGULACJE PRAWNE NORMUJĄCE FUNKCJONOWANIE OTWARTEJ BANKOWOŚCI

Ramami prawnymi dla funkcjonowania otwartej bankowości jest głównie dyrektywa PSD2[10], ustawa o usługach płatniczych[11] oraz regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji[12] (RTS).

W dalszej części publikacji przedstawiono podstawowe informacje nt. wcześniej wskazanych aktów prawnych.

2.1. DYREKTYWA PSD2

Dyrektywa PSD2 weszła w życie w dniu 13 stycznia 2016 r. i jest nowelizacją dyrektywy PSD z 2007 r., która wprowadziła zasadnicze ramy prawne dla funkcjonowania sektora usług płatniczych w całej Unii Europejskiej. Kraje członkowskie zostały zobligowane do wdrożenia przepisów dyrektywy PSD2 do prawa krajowego do dnia 13 stycznia 2018 r.

Celem dyrektywy PSD2 było dostosowanie przepisów unijnych do zmian wynikających z dynamicznego rozwoju rynku usług płatniczych, w szczególności w obszarze płatności elektronicznych (w tym mobilnych), oraz pojawienia się nowych rodzajów usług płatniczych (tj. usług dostępu do rachunku) świadczonych przez podmioty trzecie (TPP).

Regulacja określa zbiór jasnych i kompleksowych zasad, które znajdują zastosowanie zarówno do obecnych, jak i przyszłych dostawców usług płatniczych. Wspomniane zasady mają na celu zapewnienie, aby podmioty te mogły ze sobą konkurować na równych warunkach, co ma doprowadzić do zwiększenia wyboru, wydajności i przejrzystości usług płatniczych, jednocześnie wzmacniając zaufanie konsumentów do zharmonizowanego rynku płatności.

Dyrektywa PSD2 zmieniła dotychczasową działalność dostawców usług płatniczych, w szczególności banków, w kierunku modelu otwartej bankowości. W ciągu ostatnich kilku lat nastąpiły istotne zmiany w obszarze płatności detalicznych pod względem innowacji technologicznych. Doprowadziło to do wzrostu liczby płatności elektronicznych (w szczególności w obszarze bankowości mobilnej) oraz pojawienia się na rynku nowych graczy. Do tej pory zasadniczo tylko klienci banków mieli bezpośredni dostęp do swoich rachunków płatniczych i możliwość zlecania transakcji płatniczych. **Zgodnie z dyrektywą PSD2 filozofia dostępu do rachunków płatniczych zmieniła się znacząco, ponieważ uprawnione podmioty trzecie (TPP) mogą**

[10] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015L2366
[11] http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111991175
[12] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32018R0389

w imieniu i za zgodą klienta uzyskać dostęp do informacji o rachunku lub zlecać realizację płatności.

W dyrektywie PSD2 uregulowane zostały **2 nowe usługi płatnicze** oferowane przez TPP:
a) **usługa inicjowania płatności**;
b) **usługa dostępu do informacji o rachunku.**

Dodatkowo, dyrektywa PSD2 wprowadziła **usługę potwierdzania dostępności środków na rachunku**, która związana jest z wydawaniem instrumentów płatniczych opartych na karcie płatniczej[13].

Co do zasady, dyrektywa PSD2 powinna przyczynić się do powstawania różnych modeli współpracy banków z fintechami w ramach koncepcji otwartej bankowości. Obecnie wielu ekspertów rynku wskazuje, że szczególnie te mniejsze fintechy (startu-py) mają dużo większą zdolność do tworzenia i sprawnego wdrażania innowacyjnych rozwiązań niż wiele tradycyjnych banków (ang. *incumbents*). Jednocześnie, w przeciwieństwie do banków, mają one ograniczony dostęp do szerokiego grona klientów oraz dysponują znacznie mniejszymi zasobami.

Ponieważ intencją dyrektywy PSD2 jest pobudzenie rozwoju nowych rozwiązań płatniczych ukierunkowanych na klienta, wydaje się, że współpraca między bankami a fintechami będzie występowała coraz częściej, wpływając na wzrost zaufania wśród klientów do innowacyjnych produktów i usług. Podstawą tego partnerstwa będą dane, które można gromadzić i wykorzystywać z korzyścią dla klienta, banku i fintechu. Należy przy tym podkreślić, że warunkiem stabilnego rozwoju otwartej bankowości jest zapewnienie odpowiedniego poziomu bezpieczeństwa i ochrony konsumentów.

Zgodnie z dyrektywą PSD2 wszystkie usługi płatnicze oferowane drogą elektroniczną powinny być wykonywane w sposób bezpieczny, z użyciem technologii będących w stanie zagwarantować bezpieczne uwierzytelnianie klienta i w jak największym stopniu ograniczyć ryzyko oszustw.

2.2. USTAWA O USŁUGACH PŁATNICZYCH

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: UUP), będąca pierwotnie implementacją dyrektywy PSD, weszła w życie 24 października 2011 r. Przepisy UUP określają m.in. zasady świadczenia usług płatniczych oraz wydawania i wykupu pieniądza elektronicznego[14], jak również zasady funkcjonowania rynku krajowych transakcji płatniczych przy użyciu kart płatniczych.

[13] Szczegółowe informacje nt. nowych usług wynikających z dyrektywy PSD2 przedstawiono w rozdziale 3.
[14] UUP zawiera również przepisy wynikające z implementacji *Dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniającej dyrektywy 2005/60/WE i 2006/48/WE oraz uchylającej dyrektywę 2000/46/WE* (tzw. dyrektywy EMD2).

Zgodnie z art. 3 ust. 1 UUP przez usługi płatnicze rozumie się działalność polegającą na:

„1) *przyjmowaniu wpłat gotówki i dokonywaniu wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku;*

2) wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy:

a) przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty,

b) przy użyciu karty płatniczej lub podobnego instrumentu płatniczego,

c) przez wykonywanie usług polecenia przelewu, w tym stałych zleceń;

3) wykonywaniu transakcji płatniczych wymienionych w pkt 2, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 UUP;

4) wydawaniu instrumentów płatniczych;

5) umożliwianiu akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (acquiring);

6) świadczeniu usługi przekazu pieniężnego;

7) świadczeniu usługi inicjowania transakcji płatniczej[15]*;*

8) świadczeniu usługi dostępu do informacji o rachunku".

UUP wprowadziła zasadę, że **usługi płatnicze mogą być wykonywane jedynie przez dostawców usług płatniczych**, czyli oprócz banków także m.in. przez instytucje płatnicze, instytucje pieniądza elektronicznego, małe instytucje płatnicze czy też biura usług płatniczych. Oznacza to, że świadczenie usług płatniczych, jeśli nie jest wykonywane przez żaden z podmiotów uprawnionych (np. banki na podstawie odpowiednich postanowień statutu), wymaga uzyskania zezwolenia/rejestracji Komisji Nadzoru Finansowego (KNF).

W związku z implementacją dyrektywy PSD2 przepisy UUP zostały istotnie zmodyfikowane *Ustawą z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw* (Dz. U. z 2018 r. poz. 1075), która weszła w życie 20 czerwca 2018 r. W szczególności wprowadzone zostały ramy prawne dla funkcjonowania otwartej bankowości poprzez rozszerzenie katalogu usług płatniczych o 2 nowe typy usług:

[15] Usługa inicjowania transakcji płatniczej rozumiana jest w niniejszej publikacji jako usługa inicjowania płatności, która została opisana w rozdziale 3.1.

usługę inicjowania płatności oraz usługę dostępu do informacji o rachunku płatniczym, oraz określenie warunków wykonywania usługi potwierdzania środków na rachunku[16].

2.3. RTS

Kluczowym aktem prawnym uzupełniającym wymogi dyrektywy PSD2 jest *Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji* (RTS), które zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 13 marca 2018 r.[17]

RTS ma istotne znaczenie dla osiągnięcia celów PSD2 dotyczących zwiększenia ochrony konsumentów, promowania innowacji i poprawy bezpieczeństwa usług płatniczych w całej Unii Europejskiej. Dokument określa wymogi w zakresie stosowania silnego uwierzytelniania klienta oraz zasady komunikacji dostawców prowadzących rachunki płatnicze (np. banków) z podmiotami świadczącymi usługi dostępu do rachunku (TPP)[18].

Zgodnie z RTS każdy dostawca usług płatniczych prowadzący rachunki płatnicze dostępne online (np. bank) powinien oferować co najmniej jeden interfejs dostępowy umożliwiający bezpieczną komunikację z TPP.

Dostawcy usług płatniczych zostali zobowiązani do wdrożenia wymogów RTS **w ciągu 18 miesięcy** od daty ich wejścia w życie. Oznacza to, że RTS powinny być stosowane od dnia **14 września 2019 r.**[19], ale wymóg udostępnienia przez dostawców prowadzących rachunki dokumentacji technicznej i środowiska testowego dla utworzonego interfejsu komunikacji z TPP obowiązywał pół roku wcześniej, tj. od dnia 14 marca 2019 r.

Szczegółowe wyjaśnienia dotyczące implementacji RTS zostały przedstawione w opinii Europejskiego Urzędu Nadzoru Bankowego (EBA) z dnia 13 czerwca 2018 r.[20] oraz w innych opiniach EBA, które zostały wskazane w dalszej części publikacji[21].

---

[16] Usługa potwierdzania środków na rachunku nie stanowi odrębnej usługi płatniczej w świetle PSD2/UUP.
[17] RTS weszły w życie następnego dnia od daty ich publikacji.
[18] Ustanowienie wymogów RTS wynika z art. 98 PSD2.
[19] Zgodnie z *Komunikatem KNF z dnia 19 sierpnia 2019 r. w sprawie silnego uwierzytelniania klienta w przypadku niektórych form płatności przy użyciu instrumentów płatniczych* oraz opinią EBA z dnia 16 października 2019 r. termin na spełnienie niektórych wymogów w zakresie SCA, pod pewnymi warunkami, może zostać wydłużony. Szczegółowe informacje w tym zakresie przedstawiono w rozdziale 4.1. *Silne uwierzytelnianie klienta – Termin wdrożenia procedury SCA*.
[20] *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (EBA-Op-2018-04): https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf
[21] Patrz rozdział 4.1. *Silne uwierzytelnianie klienta*, rozdział 4.6. *Wymogi dla specjalnego interfejsu komunikacji* i rozdział 4.9. *Identyfikacja TPP z wykorzystaniem certyfikatów eIDAS*.

Dodatkowo należy zauważyć, że na stronie internetowej EBA stworzona została dedykowana sekcja pytań i odpowiedzi (ang. ***Single Rulebook Q&A***[22]), gdzie dostępne są odpowiedzi na pytania dotyczące m.in. implementowania nowych rozwiązań wynikających z dyrektywy PSD2, RTS i Wytycznych EBA.

Jednocześnie powołana została specjalna **Grupa robocza EBA ds. API** (ang. *EBA working group on APIs under PSD2*), która zajmuje się wyjaśnianiem kwestii problematycznych dotyczących implementacji RTS. W szczególności Grupa przygotowuje zestawy odpowiedzi na pytania uczestników rynku, które są publikowane na stronie internetowej EBA[23].

[22] https://eba.europa.eu/single-rule-book-qa

[23] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2

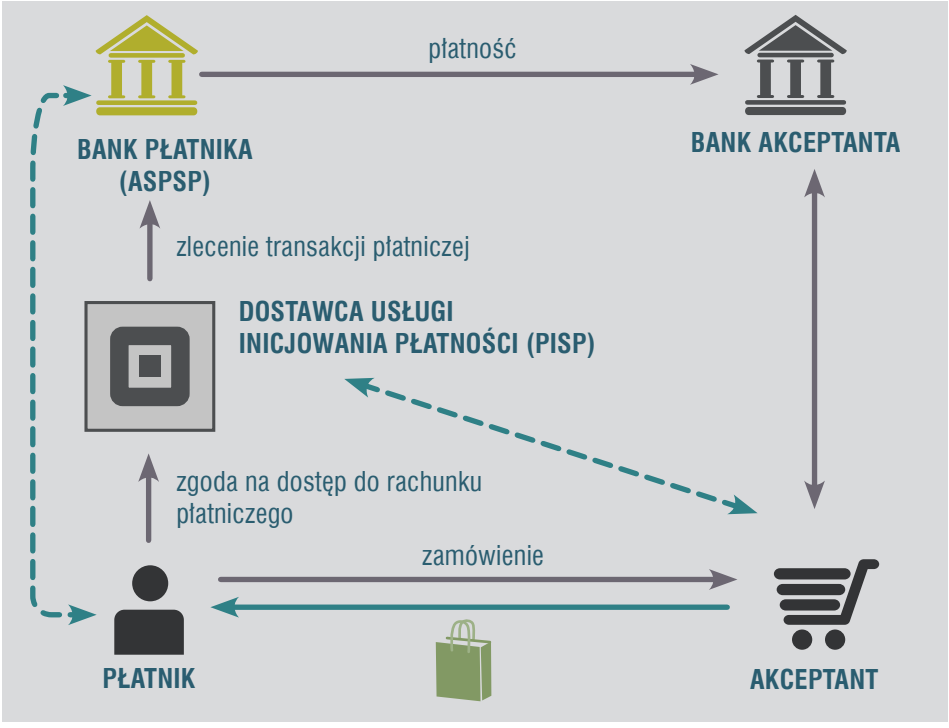
3 USŁUGI DOSTĘPU DO RACHUNKU PŁATNICZEGO

3.1. USŁUGA INICJOWANIA PŁATNOŚCI

Usługa inicjowania płatności (ang. *Payment Initiation Service* – PIS) polega na zainicjowaniu przez podmiot uprawniony do świadczenia tej usługi, na polecenie i w imieniu użytkownika, zlecenia płatniczego (polecenia przelewu) z rachunku płatniczego użytkownika dostępnego online[24].

W praktyce usługa PIS wykorzystywana jest w handlu elektronicznym, gdzie TPP jako dostawca świadczący usługę inicjowania płatności (ang. *Payment Initiation Service Provider* – PISP) wspomaga użytkownika w procesie dokonywania płatności w Internecie, nie wchodząc jednocześnie w posiadanie środków pieniężnych.

Schemat działania usługi PIS przedstawiono na rys. 1.



Rys. 1 Schemat działania usługi inicjowania płatności (PIS)
Źródło: Opracowanie własne

[24] Szczegółowe zasady świadczenia usługi PIS określone zostały w art. 59r UUP.

W przypadku chęci skorzystania z usługi PIS użytkownik, rozumiany jako płatnik, po złożeniu zamówienia w sklepie internetowym (określanym akceptantem) zostaje przekierowany na stronę PISP, gdzie jest poproszony o wskazanie dostawcy prowadzącego jego rachunek (ang. *Account Servicing Payment Service Provider* – ASPSP, bank płatnika), z którego będzie inicjowana płatność[25]. Następnie PISP, za wyraźną zgodą użytkownika, uzyskuje dostęp do konta bankowości elektronicznej użytkownika[26], gdzie uzupełnia wszystkie dane niezbędne do zlecenia płatności[27], po czym prosi użytkownika o zatwierdzenie dyspozycji wykonania przelewu na rachunek odbiorcy płatności (akceptanta). Po zatwierdzeniu realizacji transakcji przez bank płatnika PISP informuje niezwłocznie akceptanta, że płatność została zainicjowana, po czym akceptant rozpoczyna proces realizacji zamówienia i dostarcza użytkownikowi zamawiany towar lub usługę.

W świetle wymogów PSD2/UUP[28] przed zainicjowaniem płatności PISP jest zobowiązany dostarczyć lub udostępnić użytkownikowi:
1) wyszczególnienie informacji, które muszą być dostarczone przez użytkownika, aby zlecenie płatnicze mogło zostać prawidłowo zainicjowane lub wykonane;
2) informację o maksymalnym czasie wykonania usługi PIS;
3) informację o wszelkich opłatach należnych PISP, wraz ze wskazaniem kwot tych opłat;
4) informację o kursie walutowym, który będzie zastosowany do transakcji płatniczej, jeżeli transakcja płatnicza wiąże się z przeliczaniem waluty;
5) nazwę (firmę) PISP, adres siedziby oraz adres głównego miejsca wykonywania działalności, a w przypadku korzystania z usług agenta lub wykonywania działalności przez oddział w państwie członkowskim, w którym usługa jest oferowana – także adres tego agenta lub oddziału, oraz inne dane kontaktowe mające znaczenie dla celów porozumiewania się z PISP, w tym adres poczty elektronicznej;
6) dane kontaktowe właściwego organu nadzoru;
7) inne informacje uzgodnione pomiędzy PISP a użytkownikiem.

Po złożeniu zlecenia płatniczego PISP, zgodnie z PSD2/UUP[29], niezwłocznie dostarcza lub udostępnia płatnikowi, a w razie potrzeby odbiorcy:
1) potwierdzenie prawidłowego złożenia zlecenia płatniczego w systemie ASPSP;
2) numer identyfikacyjny umożliwiający płatnikowi i odbiorcy zidentyfikowanie transakcji płatniczej, a w razie potrzeby umożliwiający odbiorcy zidentyfikowanie płatnika, oraz inne informacje przekazane wraz z transakcją płatniczą;

[25] Zgodnie z art. 59r ust. 5 UUP korzystanie przez użytkownika z usługi PIS nie może być uzależnione od istnienia stosunku umownego między PISP a ASPSP.
[26] W myśl art. 59r ust. 3 pkt 2 UUP, PISP jest zobowiązany zapewnić, aby indywidualne dane uwierzytelniające użytkownika (np. hasło do systemu bankowości elektronicznej) nie były dostępne dla podmiotów innych niż użytkownik i ASPSP oraz aby były one przekazywane za pośrednictwem bezpiecznych i wydajnych kanałów.
[27] PISP nie może żądać od użytkownika innych danych niż te, które są niezbędne do wykonania usługi. Danych, które pozyskał w związku z realizacją usługi, nie może również wykorzystywać do innych celów. Ponadto PISP nie może zmieniać kwoty, odbiorcy ani innych danych dotyczących transakcji.
[28] Art. 23 UUP.
[29] Art. 59q UUP.

3) informację o kwocie transakcji płatniczej oraz łącznej kwocie opłat należnych z tytułu transakcji płatniczej na rzecz PISP, a w stosownych przypadkach wraz z wyszczególnieniem kwot tych opłat.

Ponadto PISP po złożeniu zlecenia płatniczego udostępnia ASPSP numer identyfikacyjny danej transakcji.

Jednocześnie należy wskazać, że **w przypadku nieautoryzowanej transakcji wykonanej w ramach usługi PIS, zgodnie z PSD2/UUP[30], odpowiedzialnym za zwrot użytkownikowi kwoty tej transakcji jest ASPSP**, który powinien to zrobić bezzwłocznie, a w każdym razie nie później niż do końca następnego dnia roboczego i przywrócić obciążony rachunek płatniczy użytkownika do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Jeżeli PISP jest odpowiedzialny za nieautoryzowaną transakcję płatniczą, niezwłocznie powinien zrekompensować ASPSP, na jego wniosek, straty poniesione lub sumy zapłacone w wyniku dokonania zwrotu na rzecz płatnika, łącznie z kwotą nieautoryzowanej transakcji płatniczej. Zgodnie z PSD2/UUP[31] na PISP spoczywa ciężar udowodnienia, że – w zakresie jego właściwości – transakcja płatnicza została autoryzowana, prawidłowo zapisana w systemie PISP służącym do obsługi transakcji płatniczych i że na transakcję płatniczą nie miała wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą, za którą ten dostawca odpowiada.

Warunki świadczenia usługi PIS przez krajową instytucję płatniczą

Usługa PIS, w świetle przepisów PSD2/UUP[32], traktowana jest jako **usługa płatnicza**, na świadczenie której wymagane jest posiadanie **zezwolenia KNF** na prowadzenie działalności w charakterze krajowej instytucji płatniczej (KIP). Jednocześnie należy wskazać, że zakres działalności KIP może być dużo szerszy niż świadczenie tylko samej usługi PIS.

Poniżej wskazano możliwy zakres działalności KIP w zakresie świadczenia usług płatniczych[33]:

- ✓ przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku;
- ✓ wykonywanie transakcji płatniczych, m.in. poprzez wykonywanie usług polecenia zapłaty, polecenia przelewu lub przy użyciu karty płatniczej, w tym w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu;
- ✓ wydawanie instrumentów płatniczych[34];
- ✓ acquiring;

[30] Art. 44 ust. 3a UUP.
[31] Art. 45 ust. 1a UUP.
[32] Art. 3 ust. 1 pkt 7 UUP.
[33] Szczegółowy katalog usług płatniczych określonych w UUP przedstawiono w rozdziale 2.2.
[34] W ramach usługi wydawania instrumentów płatniczych KIP może świadczyć usługę CAF (patrz rozdział 3.3.).

- ✓ usługa przekazu pieniężnego;
- ✓ usługa inicjowania transakcji płatniczej;
- ✓ usługa dostępu do informacji o rachunku[35].

Należy przy tym zaznaczyć, że KIP, w zależności od zakresu uzyskanego zezwolenia, może podejmować szereg czynności dodatkowych ściśle powiązanych ze świadczeniem usług płatniczych (np. wymianę walut, usługi bezpiecznego przechowywania środków pieniężnych przekazanych w celu wykonania transakcji płatniczej, usługi przechowywania i przetwarzania danych, prowadzenie systemów płatności, wydawanie pieniądza elektronicznego[36]), jak również prowadzić inną działalność gospodarczą w formie hybrydowej krajowej instytucji płatniczej. KIP może również świadczyć usługi płatnicze za pośrednictwem agenta wpisanego do rejestru KNF lub poprzez oddział, a także powierzyć innemu przedsiębiorcy wykonywanie określonych czynności operacyjnych związanych ze świadczeniem usług płatniczych.

Dużą zaletą wynikającą z prowadzenia działalności w formie KIP jest możliwość notyfikowania świadczonych usług w innych krajach członkowskich Unii Europejskiej w ramach tzw. **jednolitego paszportu europejskiego**[37]. Jest to szczególnie istotne z punktu widzenia koncepcji otwartej bankowości, której podstawowym założeniem funkcjonowania jest budowa rozległej sieci powiązań biznesowych pomiędzy różnymi uczestnikami rynku na rzecz rozwoju innowacyjnych produktów i usług finansowych.

Aby uzyskać zezwolenie KNF na prowadzenie działalności w charakterze KIP, należy w szczególności[38]:
- ✓ posiadać kapitał założycielski w wysokości od 20 000 do 125 000 euro, w zależności od rodzaju świadczonych usług[39];
- ✓ posiadać fundusze własne nie niższe niż kapitał założycielski;
- ✓ wprowadzić system zarządzania ryzykiem i kontroli wewnętrznej, odpowiedni do rodzaju, skali i stopnia złożoności świadczonych usług płatniczych, wraz z odpowiednimi procedurami wewnętrznym;
- ✓ przedstawić program działalności i plan finansowy na okres co najmniej 3-letni;
- ✓ stosować wymagane prawem zasady ochrony środków pieniężnych przyjętych na poczet wykonania transakcji płatniczej;
- ✓ wypełniać obowiązki instytucji obowiązanych, wynikające z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;
- ✓ wprowadzić procedury rozpatrywania skarg użytkowników;

---

[35] Informacje o usłudze AIS przedstawiono w rozdziale 3.2.

[36] Średnia wartość pieniądza elektronicznego pozostającego w obiegu wydawanego przez KIP obliczona na dany miesiąc kalendarzowy nie może przekraczać równowartości w walucie polskiej kwoty 5 000 000 euro ustalonej przy zastosowaniu kursu średniego ogłoszonego przez Narodowy Bank Polski obowiązującego w ostatnim dniu miesiąca poprzedzającego ten miesiąc (art. 73a ust. 4 UUP).

[37] W takiej sytuacji KNF zawiadamia właściwy organ nadzoru w innym państwie Unii Europejskiej, w którym KIP planuje prowadzić działalność.

[38] Szczegółowe warunki uzyskania zezwolenia na prowadzenie działalności w charakterze KIP określono w art. 64 ust.1 UUP.

[39] W celu świadczenia usługi PIS minimalny kapitał założycielski wynosi 50 000 euro.

- ✓ wykazać, że osoby zarządzające KIP posiadają odpowiednie doświadczenie zawodowe, wiedzę oraz wykształcenie w celu zarządzania działalnością w zakresie usług płatniczych;
- ✓ posiadać ubezpieczenie odpowiedzialności cywilnej, gwarancję bankową, gwarancję ubezpieczeniową lub inne zabezpieczenie roszczeń użytkownika (dotyczy tylko usługi PIS[40]);
- ✓ spełniać wymogi określone w RTS.

W praktyce warunkiem uzyskania zezwolenia KNF na prowadzenie działalności w charakterze KIP jest złożenie do organu nadzoru kompletnego wniosku zawierającego wszystkie wskazane w art. 61 ust. 1 UUP dokumenty i informacje[41], które są poddawane ocenie KNF pod kątem formalnoprawnym i merytorycznym. KNF wydaje decyzję w przedmiocie zezwolenia w terminie **3 miesięcy** od dnia otrzymania wniosku lub jego uzupełnienia. Oznacza to, że termin 3 miesięcy liczony jest od dnia, kiedy wpłynął do KNF kompletny wniosek (ewentualnie ostatni dokument uzupełniający wniosek w taki sposób, że wniosek należy uznać za kompletny). Termin rozpatrzenia sprawy może wydłużyć się zatem o czas niezbędny do uzupełnienia przez wnioskodawcę dokumentacji załączonej do wniosku. Postępowanie w przedmiocie zezwolenia na świadczenie usług płatniczych kończy się wydaniem decyzji administracyjnej zezwalającej na świadczenie usług płatniczych w charakterze KIP albo odmawiającej takiego zezwolenia.

3.2. USŁUGA DOSTĘPU DO INFORMACJI O RACHUNKU

Usługa dostępu do informacji o rachunku (ang. *Account Information Service* – AIS) polega na dostarczaniu przez podmiot uprawniony do świadczenia tej usługi, na polecenie i za zgodą użytkownika, skonsolidowanych informacji dotyczących rachunku lub rachunków płatniczych użytkownika dostępnych online prowadzonych przez jednego lub wielu innych dostawców usług płatniczych[42].

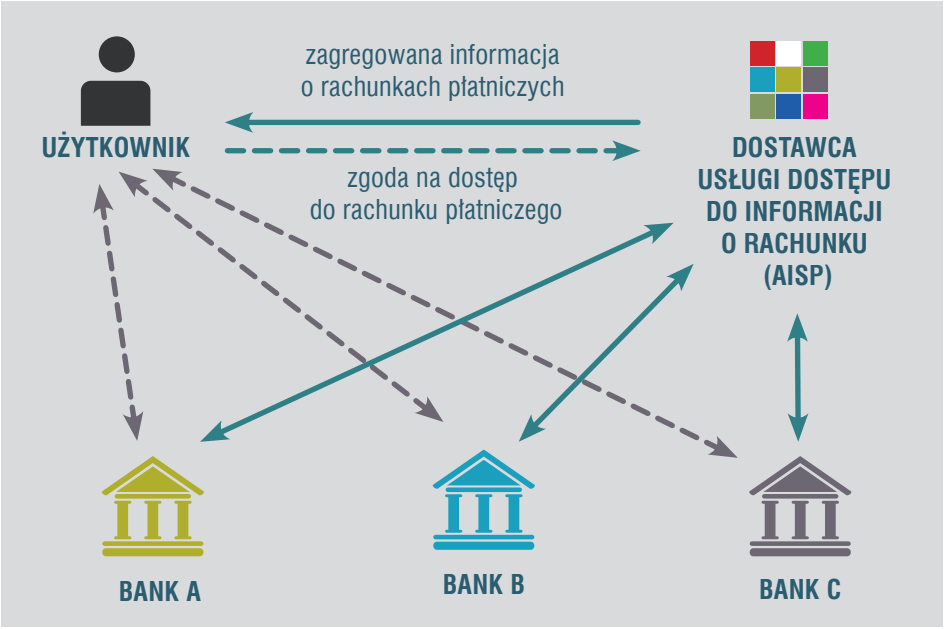
Schemat działania usługi AIS przedstawiono na rys. 2.

---

[40] Sposób obliczania minimalnego poziomu zabezpieczenia finansowego dla dostawcy PIS określono w Rozporządzeniu Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 61b ust. 1 ustawy o usługach płatniczych: http://www.dziennikustaw.gov.pl/du/2019/1459/1

[41] W ramach przygotowywania dokumentów i informacji dołączanych do wniosku o uzyskanie zezwolenia na prowadzenie działalności w charakterze KIP należy dodatkowo uwzględnić wymogi określone w rozdziale 4.1 Wytycznych EBA z dnia 8 listopada 2017 r. (EBA/GL/2017/09): http://www.eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PL.pdf/06b0a678-eccb-4d58-8268-e0e22b0c3c23
Jednocześnie należy podkreślić, że zgodnie z art. 61 ust. 3 UUP Minister Finansów określi w drodze rozporządzenia szczegółowy zakres informacji oraz rodzaj i formę dokumentów dołączanych do wniosku o wydanie zezwolenia na prowadzenie działalności w charakterze KIP, które uwzględni ww. Wytyczne EBA.

[42] Szczegółowe zasady świadczenia usługi AIS określone zostały w art. 59s UUP.



Rys. 2 Schemat działania usługi dostępu do informacji o rachunku (AIS)
Źródło: Opracowanie własne

W ramach usługi AIS użytkownik, który posiada rachunki płatnicze dostępne online w kilku bankach lub innych ASPSP, może zlecić TPP, tj. dostawcy świadczącemu usługę dostępu do informacji o rachunku (ang. *Account Information Service Provider* – AISP), przygotowanie zbiorczej informacji dotyczącej np. sald i obrotów na poszczególnych rachunkach. W tym celu AISP, na zlecenie użytkownika i za jego zgodą, uzyskuje dostęp do rachunków użytkownika za pośrednictwem bankowości elektronicznej[43], po czym agreguje i przedstawia użytkownikowi wszystkie potrzebne informacje. Użytkownik ma zatem natychmiastowy dostęp do informacji o jego aktualnej sytuacji finansowej, wpływach i obrotach na poszczególnych rachunkach.

Oferowanie usług dodatkowych na bazie usługi AIS

Usługa AIS może stanowić podstawę do budowania wielu różnych modeli działalności. Oprócz standardowej usługi, polegającej na agregacji informacji o rachunku, wskazać można kilka innych usług dodatkowych (tzw. **usług premium**), niepodlegających przepisom UUP, które mogą być rozwijane na bazie usługi AIS[44], np.:

[43] Zgodnie z art. 59s ust. 4 UUP korzystanie przez użytkownika z usługi AIS nie może być uzależnione od istnienia stosunku umownego między AISP a ASPSP.
[44] Patrz również rozdział 8. *Perspektywy rozwoju otwartej bankowości w polskim sektorze FinTech – Banki jako TPP*, w którym poruszono kwestię dopuszczalnego zakresu usług dodatkowych świadczonych przez banki.

a) *Analiza wydatków i efektywne zarządzanie domowym budżetem*
Transakcje kartowe, przelewy i polecenia zapłaty mogą być automatycznie skanowane w celu identyfikacji podobnych lub okresowych transakcji. Sumy wybranych kategorii wydatków są następnie zbiorczo prezentowane użytkownikowi, co może pomóc w bieżącym zarządzaniu domowym budżetem i planowaniu przyszłych wydatków.

b) *Wspieranie procesu oceny zdolności kredytowej*
Przy ubieganiu się o kredyt/pożyczkę, użytkownik, zamiast dostarczania kredytodawcy lub pożyczkodawcy zaświadczenia o zarobkach, może pozwolić AISP (którym jest kredytodawca/pożyczkodawca lub jego partner biznesowy) na dostęp do rachunku użytkownika w celu zweryfikowania posiadanych dochodów. Na podstawie uzyskanych danych podmiot, który ma udzielić kredytu/pożyczki, otrzymuje szeroki obraz sytuacji finansowej potencjalnego kredytobiorcy/pożyczkobiorcy i może mu nadać odpowiedni *scoring* kredytowy (ocenę punktową).

c) *Potwierdzanie tożsamości użytkownika*
Przy zdalnym zamawianiu usług przez Internet, gdzie wymagane jest potwierdzenie tożsamości użytkownika (np. zakup polisy ubezpieczeniowej, otwieranie rachunku bankowego), jego tożsamość może zostać potwierdzona za pośrednictwem AISP.

d) *Porównywarka finansowa*
Dane transakcyjne i behawioralne użytkownika pozyskane w ramach usługi AIS mogą być wykorzystywane przez porównywarki finansowe w celu wyszukiwania produktów i usług finansowych ściśle dopasowanych do jego potrzeb.

Warunki świadczenia usługi AIS przez dostawcę świadczącego wyłącznie usługę AIS

W świetle przepisów PSD2/UUP[45] usługa AIS traktowana jest jako **usługa płatnicza**, na świadczenie której, bez wykonywania innych usług płatniczych, wymagany jest wpis do właściwego rejestru KNF. Do świadczenia tylko samej usługi AIS, zgodnie z UPP, uprawniony jest *dostawca świadczący wyłącznie usługę dostępu do informacji o rachunku* (AISP).

Działalność w charakterze AISP jest działalnością regulowaną w rozumieniu przepisów *Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* (Dz. U. z 2018 r. poz. 646, z późn. zm.), co oznacza w szczególności, że podjęcie tej działalności wymaga uprzedniego uzyskania **wpisu do rejestru KNF** prowadzonego dla dostawców usług płatniczych i wydawców pieniądza elektronicznego. Podjęcie działalności w charakterze AISP nie wymaga natomiast uzyskania zezwolenia KNF. Za dzień rozpoczęcia działalności w charakterze AISP uważa się dzień dokonania wpisu do rejestru.

[45] Art. 3 ust. 1 pkt 8 UUP.

Wniosek o wpis do rejestru KNF na świadczenie usługi AIS zawiera m.in.[46]:

- ✓ podstawowe dane wnioskodawcy i prowadzonej działalności;
- ✓ statut, akt założycielski lub umowę – w przypadku spółki – albo odpis z Centralnej Ewidencji Informacji o Działalności Gospodarczej (CEIDG);
- ✓ opis struktury organizacyjnej i stosowanych procedur wewnętrznych, w szczególności zasad zarządzania ryzykiem oraz zasad przeprowadzania audytu wewnętrznego;
- ✓ program działalności i plan finansowy na okres co najmniej 3-letni;
- ✓ dokument potwierdzający posiadanie ubezpieczenia odpowiedzialności cywilnej z tytułu prowadzenia odpowiedniej działalności gospodarczej, gwarancji bankowej, gwarancji ubezpieczeniowej lub innego zabezpieczenia roszczeń użytkowników[47];
- ✓ oświadczenie o kompletności i zgodności z prawdą danych zawartych we wniosku, znajomości i spełnianiu warunków wykonywania działalności w charakterze AISP oraz świadomości odpowiedzialności karnej za złożenie fałszywego oświadczenia.

KNF jest zobowiązana dokonać wpisu AISP do rejestru w terminie **3 miesięcy** od dnia wpływu do KNF kompletnego wniosku o wpis, tj. zawierającego wszystkie wymagane dokumenty i informacje[48]. Po dokonaniu wpisu AISP do rejestru KNF z urzędu wydaje zaświadczenie o wpisie, które przesyłane jest do danego AISP.

Na podstawie uzyskanego wpisu do rejestru KNF AISP może świadczyć usługę dostępu do informacji o rachunku:

1) na terytorium Rzeczypospolitej Polskiej samodzielnie (w tym przez oddziały) lub za pośrednictwem agentów oraz
2) na terytorium państwa członkowskiego innego niż Rzeczypospolita Polska przez oddział, w ramach działalności transgranicznej (tj. bez fizycznej obecności w innym państwie członkowskim) lub za pośrednictwem agenta, po przeprowadzeniu procedury notyfikacyjnej.

AISP może również prowadzić działalność gospodarczą inną niż świadczenie usługi AIS i niezwiązaną z usługami płatniczymi (w takim przypadku AISP działa jako tzw. hybrydowy AISP).

---

[46] Szczegółowe warunki uzyskania wpisu do rejestru KNF na świadczenie wyłącznie usługi AIS określono w art. 117b UUP.

[47] Zasady obliczania minimalnego poziomu zabezpieczenia finansowego dla AISP określono w *Rozporządzeniu Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 117a ust. 3 ustawy o usługach płatniczych*: http://www.dziennikustaw.gov.pl/du/2019/1458/1

[48] W ramach przygotowywania dokumentów i informacji dołączanych do wniosku o wpis do rejestru jako AISP należy uwzględnić wymogi określone w rozdziale 4.2. Wytycznych EBA z dnia 8 listopada 2017 r. (EBA/GL/2017/09): http://www.eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PL.pdf/06b0a678-eccb-4d58-8268-e0e22b0c3c23

Jeżeli AISP zamierza świadczyć **dodatkowe usługi płatnicze**, oprócz usługi AIS, to musi posiadać **zezwolenie KNF** na prowadzenie działalności w charakterze krajowej instytucji płatniczej (KIP[49]).

Zgoda użytkownika na świadczenie usługi AIS

Świadczenie usługi AIS możliwe jest tylko za **wyraźną zgodą użytkownika**, który powinien być świadomy, komu i w jakim zakresie udziela zgody. Przed wyrażaniem zgody na wykonanie usługi AIS użytkownik powinien dokładnie przeczytać warunki świadczenia usługi (np. regulamin usługi lub umowę), w tym także uzyskać wszelkie wyjaśnienia na temat:

1) podmiotu świadczącego usługę AIS, w szczególności czy posiada on zgodę organu nadzoru na wykonywanie tego typu usługi;
2) bezpieczeństwa gromadzonych danych o użytkowniku, m.in. czy AISP stosuje przepisy wynikające z Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz czy pozyskane informacje są przekazywane dalej innym podmiotom, np. firmom technologicznym, które współpracują z AISP;
3) charakteru usługi (np. agregacji informacji o rachunku, saldzie, wykonanych transakcjach płatniczych itp.);
4) opłat należnych AISP od użytkownika, wraz z wyszczególnieniem kwot tych opłat,
5) zakresu udzielanej zgody na świadczenie usługi (m.in. rodzaju agregowanych transakcji, zakresu przetwarzanych informacji o transakcjach, np. imię i nazwisko/nazwa właściciela rachunku, numer rachunku, kwota transakcji, tytuł przelewu, data transakcji itp.);
6) okresu, na jaki zgoda została udzielona, oraz częstotliwości pobierania danych o rachunku, w szczególności czy zgoda jest udzielana jednorazowo, czy bezterminowo, a także jak często AISP jest uprawniony do dostępu do informacji o rachunku;
7) trybu odwoływania zgody użytkownika/rezygnacji z usługi[50].

Forma przedstawiania użytkownikowi informacji o usłudze AIS jest niezwykle istotna i powinna być jak najbardziej czytelna, aby mógł on dokładnie zapoznać się ze wszystkimi warunkami świadczenia usługi, zanim zacznie z niej korzystać.

Należy przy tym podkreślić, że ani regulacje, ani organ nadzoru nie zwalniają użytkownika z odpowiedzialności za jego decyzje i za to, na co wyraża zgodę. Dlatego w każdym przypadku użytkownik powinien dokładnie zapoznać się z treścią akceptowanych regulaminów czy umów na świadczenie danej usługi.

Zgodnie z przepisami PSD2/UUP[51] informacje o rachunku uzyskane przez AISP na podstawie zgody użytkownika, w ramach świadczenia usług AIS, nie mogą być używane ani przechowywane przez AISP do celów innych niż wykonanie tej usługi.

[49] Informacje dotyczące podejmowania działalności w formie KIP przedstawiono w rozdziale 3.1.
[50] Należy pamiętać, że przepisy prawa nie przewidują odwołania zgody użytkownika za pośrednictwem ASPSP.
[51] Art. 59s ust. 2 pkt 6 UUP.

Oznacza to, że w przypadku gdy AISP oferuje użytkownikom usługi dodatkowe (tzw. usługi premium), np. monitorowanie wydatków i efektywne zarządzanie domowym budżetem, to powinien on wyraźnie wskazać, że będzie ona świadczona dodatkowo w stosunku do usługi AIS. W takiej sytuacji użytkownik powinien wyrazić odrębną zgodę na taką usługę i zaakceptować poświęcony tej usłudze regulamin lub zawrzeć stosowną umowę z AISP.

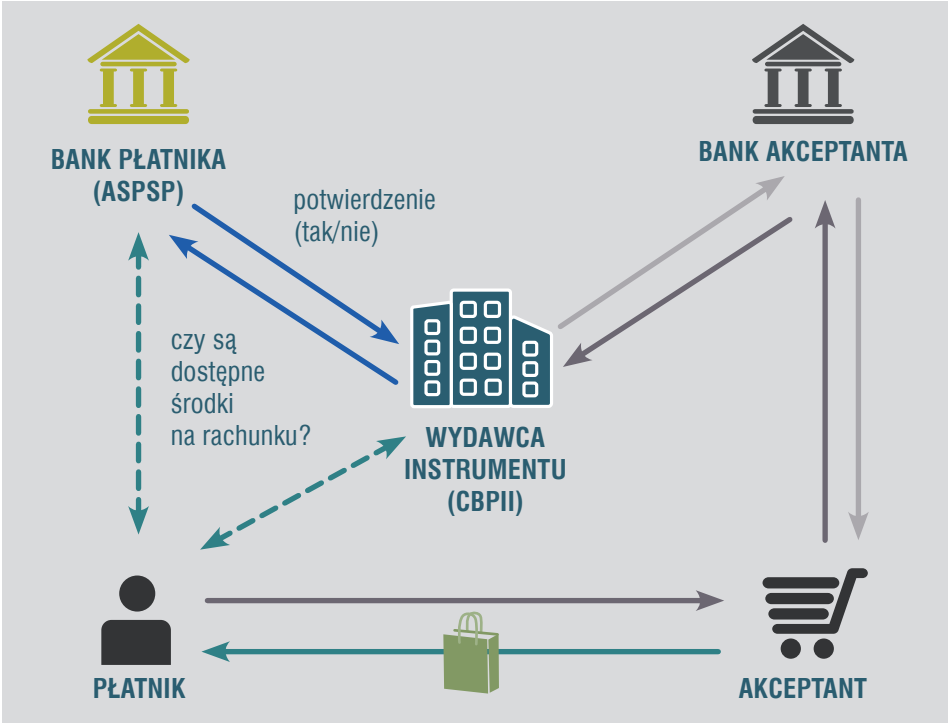
Oprócz powyższego należy również wskazać, że **w sytuacji, gdy za zgodą użytkownika dane o jego rachunkach płatniczych zostaną przekazane przez ASPSP do AISP i z jakichś powodów zostaną one później ujawnione (np. wyciek danych w wyniku ataku hakerskiego), to pełną odpowiedzialność za szkody wyrządzone użytkownikowi z tego tytułu ponosi AISP**. Należy bowiem zauważyć, że zgodnie z art. 105 ust. 1 pkt 1h *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* bank ma obowiązek udzielenia AISP informacji stanowiących tajemnicę bankową w zakresie niezbędnym do świadczenia usługi AIS. Jednocześnie treść art. 105 ust. 6 powyższej ustawy stanowi, iż bank nie ponosi odpowiedzialności za szkodę wynikającą z ujawnienia tajemnicy bankowej przez osoby i instytucje upoważnione przez ustawę do żądania od banków udzielania informacji stanowiących tajemnicę bankową. Analogiczne przepisy zostały również zawarte w art. 9f ust. 1 2b oraz art. 9f ust.4 *Ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych,* gdzie kasa jest zobowiązana udzielić AISP informacji stanowiących tajemnicę zawodową w zakresie niezbędnym do świadczenia usługi AIS, lecz nie ponosi odpowiedzialności za szkodę wynikającą z ujawnienia tajemnicy zawodowej przez osoby lub podmioty, którym kasa udzieliła informacji stanowiących tajemnicę zawodową na podstawie przepisów ww. ustawy.

3.3. USŁUGA POTWIERDZANIA DOSTĘPNOŚCI ŚRODKÓW NA RACHUNKU

Usługa potwierdzania środków na rachunku (ang. *Confirmation on Availability of Funds – CAF*) polega na umożliwieniu użytkownikowi dokonywania płatności instrumentem płatniczym opartym na karcie (np. kartą debetową), wydanym przez inny podmiot niż ten, który prowadzi rachunek płatniczy użytkownika dostępny online. W takiej sytuacji użytkownik zawiera umowę z podmiotem uprawnionym do świadczenia usługi CAF, który dostarcza użytkownikowi instrument płatniczy bez konieczności otwierania dodatkowego rachunku, gdyż instrument ten będzie powiązany z rachunkiem płatniczym, który został już przez użytkownika założony u pierwotnego dostawcy i z tego rachunku będą pobierane środki w przypadku dokonywania płatności[52].

Schemat działania usługi CAF przedstawiono na rys. 3.

[52] Szczegółowe zasady świadczenia usługi CAF zostały określone w art. 49a UUP.



Rys. 3 Schemat działania usługi potwierdzania dostępności środków na rachunku (CAF)

Źródło: Opracowanie własne

Po zainicjowaniu przez płatnika zlecenia płatniczego TPP jako wydawca instrumentu płatniczego opartego na karcie, świadczący usługę potwierdzania dostępności środków na rachunku (ang. *Card-Based Payment Instrument Issuer* – CBPII), występuje, na podstawie otrzymanej zgody użytkownika, z wnioskiem do dostawcy prowadzącego dla użytkownika rachunek płatniczy (ASPSP – bank płatnika) o potwierdzenie dostępności środków na rachunku w kwocie równej zleconej płatności. W odpowiedzi ASPSP przekazuje do CBPII **krótki komunikat („TAK" lub „NIE")**, czy wymagana kwota jest dostępna, bez wskazywania wysokości salda na tym rachunku. Należy przy tym pamiętać, że zgodnie z PSD2/UUP[53] potwierdzenie dostępności środków na rachunku nie umożliwia ASPSP dokonania blokady tych środków na rachunku płatniczym płatnika. Oznacza to, że **w niektórych sytuacjach może istnieć potencjalne ryzyko braku środków na rachunku użytkownika w momencie rozliczania płatności przez CBPII**.

Przy rozliczeniu płatności w ramach usługi CAF dochodzi zazwyczaj do dwóch transakcji: pierwsza transakcja odbywa się między CBPII a bankiem akceptanta, natomiast druga – będąca zwykle poleceniem zapłaty – odbywa się między ASPSP a CBPII.

[53] Art. 49a ust. 4 UUP.

Obie transakcje powinny być traktowane tak samo jak wszelkie inne równoważne transakcje.

Przed skorzystaniem z usługi płatnik jest zobowiązany udzielić wcześniejszej zgody:
a) ASPSP w zakresie odpowiadania na wnioski CBPII dotyczące otrzymania informacji o dostępności środków;
b) CBPII w zakresie występowania z wnioskiem do ASPSP o potwierdzenie dostępności środków.

Warunki świadczenia usługi CAF

Biorąc pod uwagę katalog usług płatniczych wskazanych w PSD2/UUP[54], usługa CAF może być wykonywana w ramach **usługi wydawania instrumentów płatniczych**[55], z tą różnicą, że instrumenty powiązane są z rachunkiem prowadzonym przez innego dostawcę usług płatniczych. Oznacza to, że w celu wykonywania usługi CAF niezbędne jest posiadanie **zezwolenia KNF** na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej (KIP[56]), chyba że usługa ta byłaby świadczona przez uprawniony do tego podmiot, np. bank, na podstawie odpowiednich postanowień w statucie.

[54] Art. 3 ust. 1 UUP.
[55] W zależności od modelu biznesowego, w celu świadczenia usługi wydawania instrumentów płatniczych, niezbędne może być również świadczenie innych usług płatniczych, takich jak np. prowadzenie rachunku płatniczego lub wykonywanie transakcji płatniczych.
[56] Informacje dotyczące podejmowania działalności w formie KIP przedstawiono w ramach rozdziału 3.1.

4 KLUCZOWE WYMOGI RTS

Przepisy RTS nałożyły na dostawców usług płatniczych szereg różnych obowiązków dotyczących stosowania silnego uwierzytelniania klienta oraz bezpiecznych standardów komunikacji w zakresie świadczenia usług dostępu do rachunku. W dalszej części publikacji opisano wymogi RTS, które wydają się istotne z punktu widzenia rozwoju otwartej bankowości.

4.1. SILNE UWIERZYTELNIANIE KLIENTA

Sam wymóg stosowania silnego uwierzytelniania klienta wynika z PSD2/UUP, natomiast w RTS zawarto przepisy uszczegóławiające, które zostały omówione w dalszej części publikacji[57].

Na wstępie należy wskazać kilka istotnych definicji wynikających z PSD2/UUP, które są kluczowe do zrozumienia wymogów RTS w zakresie silnego uwierzytelniania klienta:

Uwierzytelnianie (ang. *authentication*) – procedura umożliwiająca dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika.

Indywidualne dane uwierzytelniające (ang. *personalised security credential*) – indywidualne dane zapewniane przez dostawcę usług płatniczych użytkownikowi usług płatniczych do celów uwierzytelniania (np. hasło do systemu bankowości elektronicznej).

Silne uwierzytelnianie klienta (ang. *strong customer authentication*, skrót: SCA) – uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do różnych, spośród 3, kategorii:
- **wiedza** – „coś", co zna tylko użytkownik (np. PIN, hasło wielorazowe, tajne pytanie i odpowiedź, wzór na ekranie smartfona – tzw. wężyk),
- **posiadanie** – „coś", co tylko użytkownik posiada (np. smartfon z kartą SIM przypisaną do numeru telefonu użytkownika lub odpowiednia aplikacja w smartfonie),

[57] Przed uchwaleniem dyrektywy PSD2 stosowanie silnego uwierzytelniania klienta było przedmiotem rekomendacji nadzorczych wydawanych m.in. przez ECB (*The European Forum on the Security of Retail Payments – SecuRe Pay*), EBA i KNF.

– **cecha użytkownika** – „coś", czym użytkownik jest (unikalna cecha oparta na biometrii, np. odcisk palca, skan siatkówki oka, obraz twarzy, biometria głosu),

będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych[58].

Przepisy PSD2/UUP, ze względu na swoją neutralność technologiczną, mogą powodować pewne niejasności w zakresie wdrożenia procedury SCA przez dostawcę usług płatniczych prowadzącego rachunek (ASPSP, m.in. bank).

Z uwagi na powyższe w dniu 21 czerwca 2019 r. EBA opublikowała opinię[59], w której szczegółowo wyjaśniła, które elementy SCA są zgodne z wymogami PSD2 i do jakich kategorii należy je kwalifikować. Z przedmiotowej opinii EBA wynika, że np. kod CVV/CVC zawarty na karcie kredytowej, numer identyfikacyjny użytkownika (login) czy też adres e-mail użytkownika nie mogą być traktowane jako elementy z kategorii „wiedza", gdyż nie są one znane tylko i wyłącznie użytkownikowi, w przeciwieństwie np. do hasła lub PIN-u, które są nadawane indywidualnie przez użytkownika i nie są dostępne dla osób trzecich. Jednocześnie należy zauważyć, że EBA wspiera dalszy rozwój innowacji w sektorze finansowym i dopuszcza możliwość stosowania w ramach SCA takich danych biometrycznych, jak np. geometria dłoni, kąt trzymania urządzenia, dynamika wpisywania znaków na klawiaturze (ang. *keystroke dynamics*) czy sposób poruszania myszą komputerową.

Zgodnie z art. 32i UUP silne uwierzytelnianie klienta powinno być stosowane przez dostawców usług płatniczych, w przypadku gdy płatnik:

a) uzyskuje dostęp do swojego rachunku w trybie online (dotyczy również usługi AIS),

b) inicjuje elektroniczną transakcję płatniczą (dotyczy również usługi PIS),

c) przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć (dotyczy również usługi PIS i AIS).

Powyższe oznacza, że silne uwierzytelnianie klienta (w praktyce przeprowadzenie dodatkowej autoryzacji transakcji lub innej operacji, np. kodem SMS) powinno być stosowane w przypadku logowania się klienta do systemu bankowości elektronicznej, inicjowania płatności kartą płatniczą lub innym instrumentem płatniczym oraz płatności internetowych.

[58] SCA nazywane jest również uwierzytelnianiem dwuskładnikowym (ang. *Two-Factor Authentication* – 2FA).

[59] *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06): https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

Należy jednocześnie wskazać, że jeżeli użytkownik nie chce za każdym razem dodatkowo autoryzować dostępu do swojego rachunku, EBA dopuszcza możliwość logowania się do konta za pośrednictwem tzw. **urządzenia zaufanego** (np. komputera, smartfona lub tabletu), ale musi być ono wcześniej (przy logowaniu do konta) potwierdzone przez użytkownika jako zaufane, np. za pomocą kodu SMS, tokenu lub mobilnego podpisu[60].

Dynamiczne łączenie kodu uwierzytelniającego z kwotą i odbiorcą transakcji

W przypadku gdy użytkownik inicjuje elektroniczną transakcję płatniczą w Internecie, dostawca usług płatniczych (w tym dostawca PIS) powinien stosować silne uwierzytelnianie klienta obejmujące dodatkowo elementy, które dynamicznie łączą transakcję płatniczą z określoną kwotą transakcji oraz określonym odbiorcą (tzw. dynamiczne linkowanie, z ang. *dynamic linking*). Przykładowo w wiadomości SMS wraz z kodem autoryzacyjnym powinien być zawarty numer rachunku odbiorcy, lub jego ostatnie cyfry, i kwota transakcji. Innym rozwiązaniem może być zainstalowanie i aktywowanie odpowiedniej aplikacji mobilnej na smarfonie użytkownika, tzw. mobilna autoryzacja[61].

Odpowiedzialność za nieautoryzowane transakcje w przypadku braku stosowania SCA

Zgodnie z art. 46 ust. 4a UUP w sytuacji, gdy dostawca płatnika nie wymaga SCA, płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie. W przypadku gdy odbiorca lub dostawca odbiorcy nie akceptują SCA, odpowiadają oni za szkody poniesione przez dostawcę płatnika.

Termin wdrożenia procedury SCA

Procedura silnego uwierzytelniania klienta, zgodnie z RTS, powinna być stosowana od dnia **14 września 2019 r.** Należy jednocześnie zaznaczyć, że KNF w swoim komunikacie z dnia 19 sierpnia 2019 r.[62] zwróciła uwagę, iż zgromadzone przez EBA informacje w zakresie europejskiego rynku usług płatniczych wskazują na niedostateczne przygotowanie uczestników tego rynku do pełnego wdrożenia zasad silnego uwierzytelniania klienta przy płatnościach dokonywanych za pośrednictwem kanałów elektronicznych, w tym zwłaszcza w obszarze e-commerce. Dotyczy to nie tylko dostawców usług płatniczych, lecz także nienadzorowanych interesariuszy rynku usług płatniczych, w tym zwłaszcza odbiorców płatności (sprzedawców, merchantów). Obserwacje te potwierdzają również zgromadzone przez UKNF informacje i przeprowadzone analizy w zakresie rynku polskiego.

---

[60] Ibidem.

[61] Karty kodów jednorazowych (tzw. karty zdrapki), co do zasady, nie spełniają wymogu dynamicznego linkowania określonego w RTS.

[62] *Komunikat KNF w sprawie silnego uwierzytelniania klienta w przypadku niektórych form płatności przy użyciu instrumentów płatniczych* z dnia 19.08.2019 r.: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_KNF_w_sprawie_silnego_uwierzytelniania_klienta_66811.pdf

Uwzględniając złożoność rozwiązań stosowanych na rynkach usług płatniczych w Unii Europejskiej oraz niezbędnych zmian wymaganych do pełnego, niepowodującego zakłóceń na tych rynkach wdrożenia rozwiązań w zakresie silnego uwierzytelniania klienta, EBA, w swojej opinii z dnia 21 czerwca 2019 r.[63], stwierdziła, że na zasadzie wyjątku i w celu uniknięcia niezamierzonych negatywnych konsekwencji dla użytkowników usług płatniczych po 14 września 2019 r. **organy nadzorcze Państw Członkowskich mogą dopuścić dodatkowy, ograniczony czas na umożliwienie migracji stosowanych obecnie metod uwierzytelniania do rozwiązań w pełni zgodnych z wymogami dyrektywy PSD2**. Taka elastyczność podejścia nadzorczego wymaga jednak od poszczególnych dostawców usług płatniczych przedstawienia odpowiedniego „**planu migracji**", uzgodnienia tego planu z organem nadzoru, a także ścisłej współpracy z organem nadzoru przy realizacji tego planu.

Mając na względzie poczynione ustalenia na temat stanu gotowości uczestników polskiego rynku usług płatniczych do pełnego wdrożenia rozwiązań w zakresie silnego uwierzytelniania klienta oraz potrzebę zapewnienia, aby wdrożenie to nie powodowało zakłóceń w funkcjonowaniu tego rynku oraz niedogodności po stronie użytkowników usług płatniczych, KNF uznała za dopuszczalne zastosowanie proponowanego przez EBA rozwiązania w odniesieniu do **płatności internetowych przy wykorzystaniu karty płatniczej oraz płatności zbliżeniowych (bezstykowych)** realizowanych w terminalach płatniczych. Oznacza to, że wobec dostawców usług płatniczych, którzy **przed dniem 14 września 2019 r**. zgłosili do KNF potrzebę zastosowania powyższego rozwiązania, a następnie przedstawili stosowny, uzgodniony z KNF, realny „**plan migracji**", w okresie prawidłowej realizacji tego planu, nie będą stosowane środki nadzorcze związane z niestosowaniem silnego uwierzytelniania klienta. Podkreślić jednak należy, że nawet **w takim przypadku ryzyko związane z niestosowaniem od 14 września 2019 r. silnego uwierzytelniania klienta zgodnego z RTS w pełni obciąża zobowiązanych do tego dostawców usług płatniczych**[64].

Jednocześnie należy zauważyć, że w dniu 16 października 2019 r. EBA opublikowała opinię[65], w której wskazała, że **plany migracji dostawców usług płatniczych w zakresie dostosowania ich działalności do wymogów SCA w obszarze płatności internetowych przy wykorzystaniu kart płatniczych powinny zostać zrealizowane do dnia 31 grudnia 2020 r.**, obejmując zarówno fazę implementacji, jak również testowania rozwiązań SCA po stronie odbiorców płatności (sprzedawców, merchantów). W przedmiotowej opinii EBA określiła również **harmonogram oczekiwanych działań ze strony organów nadzoru** w związku z procesami migracji prowadzonymi przez dostawców usług płatniczych, pełniących rolę wydawców instrumentów płatniczych (ang. *issuing PSP*s) lub agentów rozliczeniowych (ang. *acquiring PSP*s).

---

[63] *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06): https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

[64] Zgodnie z art. 46 ust. 4a UUP.

[65] *Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions* (EBA-Op-2019-11): https://eba.europa.eu/documents/10180/2622242/Opinion+on+the+deadline+for+the+migration+to+SCA.pdf

Oprócz powyższego należy dodać, że w dniu 6 września 2019 r. UKNF wydał komunikat[66], w którym zwrócił uwagę, iż związana z wdrażaniem rozwiązań SCA **konieczność wzmożonych kontaktów ze strony dostawców usług płatniczych ze swoimi klientami może zostać wykorzystana przez przestępców do prób wyłudzenia poufnych informacji**, w tym poprzez przeprowadzanie ataków phishingowych, a w konsekwencji do kradzieży tożsamości lub kradzieży środków finansowych.

W związku z powyższym UKNF wskazał na konieczność zachowania szczególnej ostrożności oraz zaapelował do klientów instytucji finansowych o postępowanie zgodne z ustalonymi przez te instytucje standardami w zakresie komunikacji. W opinii UKNF uzasadnione podejrzenia powinny wzbudzać wszelkiego rodzaju wiadomości mailowe, SMS oraz próby kontaktu telefonicznego powołujące się na wejście w życie nowych rozwiązań, gdzie klient proszony jest o przekazanie informacji zawierających dane wrażliwe[67] lub informowany jest o zablokowanym rachunku albo proszony jest o kliknięcie w przesłany mailem lub SMS-em link internetowy, zmianę hasła lub innych danych do logowania za pomocą przesłanego linku internetowego, otworzenie podejrzanego załącznika, uruchomienie lub instalację przesłanej aplikacji, wykonanie podejrzanej płatności lub przelewu internetowego.

W przypadku jakichkolwiek wątpliwości UKNF zalecił klientom bezpośredni kontakt z właściwym dostawcą usług płatniczych. Jednocześnie zachęcił do zaktualizowania posiadanej wiedzy w zakresie bezpiecznego korzystania z usług finansowych poprzez odwiedzenie stron internetowych instytucji finansowych, na których zamieszczone są szczegółowe informacje i ostrzeżenia w zakresie bezpiecznego korzystania z ich usług.

Dodatkowe wymogi RTS w zakresie SCA

Analizując kwestię stosowania silnego uwierzytelniania klienta od strony technicznej, należy zauważyć, że zgodnie z art. 4 RTS przeprowadzenie procedury SCA w oparciu o zastosowanie co najmniej dwóch elementów należących do różnych, spośród trzech, kategorii: wiedza, posiadanie lub cecha klienta, powinno prowadzić do wygenerowania **kodu uwierzytelniającego**[68], który ASPSP może przyjąć wyłącznie jeden raz. Ponadto ASPSP powinien wdrożyć takie środki bezpieczeństwa, aby:

a) z ujawnionego kodu uwierzytelniającego nie było możliwe pozyskanie żadnych informacji dotyczących elementów z kategorii wiedza, posiadanie, cecha;

---

[66] *Ostrzeżenie UKNF z dnia 6 września 2019 r. dot. wyłudzania poufnych informacji w zw. z PSD2*: https://www.knf.gov.pl/o_nas/komunikaty?articleId=66987&p_id=18

[67] W szczególności dane logowania do bankowości elektronicznej, kody autoryzacyjne i kody PIN, dane osobowe.

[68] Kod uwierzytelniający jest wynikiem przeprowadzonej procedury SCA i nie może być utożsamiany z kodem autoryzacyjnym, który służy do potwierdzania przez użytkownika transakcji płatniczej lub innej operacji w ramach bankowości elektronicznej.

b) wygenerowanie nowego kodu uwierzytelniającego nie było możliwe na podstawie znajomości jakiegokolwiek innego kodu uwierzytelniającego wygenerowanego wcześniej;
c) nie można było sfałszować kodu uwierzytelniającego.

RTS wprowadza również inne dodatkowe wymogi związane z przeprowadzaniem procedury SCA, tj.:
a) brak wygenerowania kodu uwierzytelniającego nie może wskazywać, który z elementów zastosowanych w ramach silnego uwierzytelniania był błędny;
b) liczba mogących nastąpić po sobie **nieudanych prób uwierzytelnienia**, po której przekroczeniu czynność wykonywana przez użytkownika zostaje tymczasowo lub stale zablokowana, nie może przekroczyć **5 prób** w określonym okresie;
c) sesje komunikacyjne powinny być chronione przed przechwyceniem danych uwierzytelniających przekazywanych podczas uwierzytelniania oraz przed manipulacją ze strony osób niepowołanych;
d) **maksymalny czas bezczynności** użytkownika po jego uwierzytelnieniu na potrzeby dostępu do jego rachunku płatniczego w trybie online nie może przekraczać **5 minut**.

Należy również wskazać, że zgodnie z art. 9 RTS **wszystkie elementy stosowane w ramach SCA (tj. wiedza, posiadanie, cecha) powinny być niezależne od pozostałych, aby zapewnić całkowite bezpieczeństwo i poufność danych**. W szczególności dotyczy to sytuacji, w której do procedury silnego uwierzytelniania wykorzystywane jest jedno urządzenie wielofunkcyjne (np. smartfon lub tablet). W takim przypadku dostawcy usług płatniczych powinni przyjąć środki bezpieczeństwa zmniejszające ryzyko wynikające z możliwości użycia tego urządzenia wielofunkcyjnego w sposób nieuprawniony, takie jak:
a) stosowanie osobnych bezpiecznych środowisk uruchomieniowych za pośrednictwem oprogramowania zainstalowanego na urządzeniu wielofunkcyjnym;
b) mechanizmy zapewniające, aby płatnik lub osoba trzecia nie dokonali zmian w oprogramowaniu bądź urządzeniu;
c) jeżeli wprowadzono zmiany – mechanizmy łagodzące konsekwencje wprowadzonych zmian.

W przypadku stosowania SCA w ramach otwartej bankowości z udziałem TPP ASPSP powinien umożliwić dostawcy PIS i AIS świadczenie usług dostępu do rachunku w oparciu o to samo uwierzytelnianie, które jest stosowane w relacji między użytkownikiem a ASPSP. Jednocześnie należy podkreślić, że nie oznacza to, iż TPP musi wchodzić w posiadanie indywidulanych danych uwierzytelniających użytkownika[69].

[69] Patrz też rozdział 5. *Standard PolishAPI jako istotny element otwartej bankowości* – metody uwierzytelniania użytkownika.

Wyłączenia z obowiązku stosowania SCA

RTS określa nie tylko wymogi, których trzeba przestrzegać przy stosowaniu SCA, ale również sytuacje, kiedy można je pominąć, tzw. wyłączenia.

Biorąc pod uwagę zakres niniejszej publikacji, poniżej wskazano tylko te wyłączenia, które mogą mieć istotny związek z usługami dostępu do rachunku.

Zgodnie z art. 10 RTS dostawcy AIS mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem poniższych warunków, w przypadku gdy dostęp użytkownika usług płatniczych, bez ujawniania szczególnie chronionych danych dotyczących płatności[70], ogranicza się do dostępu w trybie online obejmującego:

a) **informacje o saldzie** jednego wyznaczonego rachunku płatniczego lub większej liczby wyznaczonych rachunków płatniczych i/lub
b) **informacje o transakcjach płatniczych** przeprowadzonych w ciągu ostatnich **90 dni** za pośrednictwem jednego wyznaczonego rachunku płatniczego lub większej ich liczby.

Jednocześnie należy podkreślić, że dostawcy AIS nie podlegają wyłączeniu z obowiązku stosowania SCA, jeżeli spełniony jest którykolwiek z następujących warunków:

a) użytkownik uzyskuje dostęp do powyższych informacji w trybie online **po raz pierwszy**;
b) minęło więcej niż **90 dni**, odkąd użytkownik **po raz ostatni uzyskał dostęp** w trybie online do określonych powyżej informacji w zakresie transakcji płatniczych (pkt. b) oraz odkąd **ostatni raz zastosowano SCA**.

Inne wyłączenie spod wymogu stosowania SCA, które może mieć znaczenie dla rozwoju otwartej bankowości, dotyczy **transakcji niskokwotowych**. Zgodnie z art. 16 RTS dostawcy usług płatniczych (w tym dostawcy PIS) mogą nie stosować SCA w przypadku, gdy płatnik inicjuje zdalną elektroniczną transakcję płatniczą i spełnione zostały następujące warunki:

a) kwota zdalnej elektronicznej transakcji płatniczej nie przekracza kwoty **30 euro** oraz
b) łączna kwota poprzednich zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania SCA nie przekracza kwoty **100 euro** lub
c) liczba poprzednio wykonanych zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania SCA nie przekracza **5** następujących po sobie pojedynczych zdalnych elektronicznych transakcji płatniczych.

[70] Szczególnie chronione dane dotyczące płatności (ang. *sensitive payment data*) oznaczają dane, w tym indywidualne dane uwierzytelniające, które mogą być wykorzystywane do dokonywania oszustw, z wyłączeniem imienia i nazwiska lub nazwy właściciela rachunku i numeru rachunku w przypadku działalności prowadzonej przez dostawców PIS i AIS.

Ponadto należy wskazać, że jeżeli w ramach analizy ryzyka transakcji w czasie rzeczywistym dana transakcja płatnicza jest uznawana za **transakcję niskiego ryzyka**, wówczas również możliwe jest zastosowanie wyłączenia spod wymogu SCA, przyjmując zamiast tego skuteczne procedury oparte na analizie ryzyka[71], które gwarantują bezpieczeństwo środków pieniężnych i danych osobowych użytkownika.

Podsumowując przedstawione powyżej wymogi dotyczące stosowania SCA, należy podkreślić, że ich głównym celem jest **zwiększenie poziomu bezpieczeństwa usług bankowości elektronicznej**, natomiast wyłączenia z obowiązku stosowania SCA są wynikiem kompromisu uwzględniającego potrzebę rozwoju innowacji i zapewnienia wygody klienta w procesie dokonywania płatności. W niektórych przypadkach, gdy nie jest możliwe zastosowanie wyłączenia, procedura SCA może wydłużyć czas autoryzacji transakcji lub dostępu do rachunku, ale należy pamiętać, że procesy te będą ulegać stopniowemu przyśpieszaniu z uwagi na coraz częstsze wykorzystywanie metod weryfikacji tożsamości użytkownika opartych na danych biometrycznych, na które wskazuje również europejski nadzorca – EBA.

4.2. OGÓLNE WYMOGI DLA INTERFEJSÓW KOMUNIKACJI Z TPP

Kluczowym elementem funkcjonowania otwartej bankowości jest zapewnienie przez ASPSP otwartych interfejsów programistycznych (API), na bazie których strony trzecie (TPP) mogą oferować innowacyjne produkty i usługi.

Zgodnie z art. 30 RTS każdy ASPSP, który obsługuje rachunki płatnicze dostępne online, powinien zapewnić **co najmniej jeden interfejs komunikacji z TPP** umożliwiający bezpieczną wymianę danych.

Interfejs komunikacji powinien zapewniać TPP możliwość identyfikacji wobec ASPSP. Co więcej, taki interfejs powinien umożliwić dostawcom AIS i PIS poleganie na procedurach uwierzytelniania zapewnianych przez ASPSP użytkownikowi.

Przepisy RTS wskazują, że interfejs komunikacji powinien być zbudowany w taki sposób, aby spełniał następujące wymogi:

a) dostawca usługi PIS i AIS jest w stanie zlecić ASPSP rozpoczęcie uwierzytelniania na podstawie **zgody wyrażonej przez użytkownika**;
b) sesje komunikacyjne, w których uczestniczą ASPSP, dostawca AIS, dostawca PIS i jakikolwiek zainteresowany użytkownik, ustanawia się i utrzymuje **przez cały czas trwania procesu uwierzytelniania**;

[71] Procedury bezpieczeństwa transakcji oparte na analizie ryzyka powinny uwzględniać wyniki analizy ryzyka – potwierdzające, że nie odnotowano żadnego nadzwyczajnego schematu wydatków ani wzorca zachowań ze strony płatnika, z uwzględnieniem innych czynników ryzyka, w tym informacji na temat lokalizacji płatnika i odbiorcy – w połączeniu z progami kwotowymi opartymi na wskaźnikach oszustw obliczonych dla zdalnych transakcji płatniczych zgodnie z art. 19 RTS.

c) zapewniona jest **integralność i poufność** indywidualnych danych uwierzytelniających i kodów uwierzytelniających przekazywanych przez dostawcę PIS lub dostawcę AIS lub za pośrednictwem tych dostawców.

Dodatkowo należy wskazać, że ASPSP powinien zapewnić zgodność swojego interfejsu ze standardami komunikacji publikowanymi przez **międzynarodowe lub europejskie organy normalizacyjne**.

Oprócz powyższego należy zauważyć, że zgodnie z art. 30 ust. 6 RTS właściwy organ nadzorczy (w Polsce KNF) powinien zapewnić, aby każdy ASPSP stale przestrzegał obowiązków przewidzianych w RTS w stosunku do wdrożonego interfejsu lub wdrożonych interfejsów komunikacji. W przypadku gdy ASPSP nie spełnia wymogów dotyczących interfejsów określonych w RTS, KNF podejmuje odpowiednie działania nadzorcze, aby nie doszło do powstania przeszkód i zakłóceń w świadczeniu usług PIS i AIS, o ile dostawcy tych usług spełniają warunki określone w art. 33 ust. 5 RTS[72].

4.3. SPECYFIKACJA TECHNICZNA DLA INTERFEJSU KOMUNIKACJI

Wymogi RTS określone w art. 30 ust. 3 wskazują, że ASPSP jest zobowiązany zapewnić **dokumentację** udostępnionego interfejsu komunikacji określającą zestaw procedur, protokołów i narzędzi, którego TPP potrzebują, aby umożliwić współdziałanie ich oprogramowania i aplikacji z systemami ASPSP.

W szczególności ASPSP powinien udostępnić **nieodpłatnie** dokumentację na wniosek posiadających zezwolenie dostawców PIS, AIS i CAF lub dostawców usług płatniczych, którzy złożyli wniosek do KNF o stosowne zezwolenie/rejestrację, nie później niż **6 miesięcy** przed datą 14 września 2019 r. lub przed datą docelową wprowadzenia na rynek interfejsu dostępowego oraz publicznie udostępnić streszczenie (podsumowanie) tej dokumentacji na swojej stronie internetowej.

Oprócz powyższego ASPSP powinien – z wyjątkiem sytuacji nadzwyczajnych – informować z wyprzedzeniem dostawców PIS, AIS i CAF lub dostawców usług płatniczych, którzy złożyli do KNF wniosek o stosowne zezwolenie/rejestrację, o wszelkich **zmianach w specyfikacji technicznej interfejsu** w jak najszybszym terminie i nie później niż **3 miesiące** przed wdrożeniem tych zmian.

[72] Dotyczy w szczególności warunku wprowadzenia przez dostawców PIS i AIS niezbędnych środków w celu zapewnienia, że nie przechowują oni ani nie przetwarzają posiadanych danych w celach innych niż świadczenie usług zleconych przez użytkownika. Innym warunkiem jest rejestrowanie przez dostawców PIS i AIS danych, do których dostęp uzyskali za pośrednictwem interfejsu prowadzonego przez ASPSP na potrzeby swoich użytkowników, i na wniosek, bez zbędnej zwłoki, przedstawienie plików rejestrów organowi nadzoru.

4.4. ŚRODOWISKO TESTOWE DLA INTERFEJSU KOMUNIKACJI

Każde projektowane rozwiązanie, zanim zostanie wprowadzone na rynek, musi zostać przetestowane w odpowiednim środowisku testowym. Zasada ta dotyczy również usług TPP.

Zgodnie z art. 30 ust. 5 RTS, ASPSP powinien udostępnić środowisko testowe (w tym wsparcie) służące do testowania połączenia i funkcjonalności wdrożonego interfejsu komunikacji, aby umożliwić posiadającym zezwolenie dostawcom PIS, AIS i CAF lub dostawcom usług płatniczych, którzy złożyli wniosek do organu nadzoru o stosowne zezwolenie/rejestrację, przetestowanie ich oprogramowania i aplikacji wykorzystywanych do oferowania usług płatniczych użytkownikom. Przedmiotowe środowisko testowe powinno być udostępnione nie później niż **6 miesięcy** przed datą 14 września 2019 r. lub przed datą docelową wprowadzenia na rynek interfejsu dostępowego, jeżeli data wprowadzenia na rynek była późniejsza niż data 14 września 2019 r.

Dodatkowo warto wskazać, że udostępniane środowisko testowe powinno posiadać możliwość testowania rozwiązań opartych na procedurze silnego uwierzytelniania klienta, o której mowa w rozdziale 4.1.

Należy jednocześnie podkreślić, że za pośrednictwem środowiska testowego nie może dochodzić do wymiany szczególnie chronionych danych dotyczących płatności[73].

4.5. WARIANTY INTERFEJSU KOMUNIKACJI

Kierując się zasadą neutralności technologii i modelu biznesowego, zgodnie z art. 31 RTS, ASPSP może zapewnić interfejs komunikacji z TPP poprzez:

a) **utworzenie specjalnego interfejsu komunikacji (API)**, który będzie zawierał wszystkie niezbędne informacje i funkcje dla podmiotów świadczących usługi dostępu do rachunku[74] lub
b) **modyfikację systemu bankowości internetowej** poprzez wprowadzenie możliwości identyfikowania się TPP względem ASPSP z wykorzystaniem certyfikatów eIDAS[75]. Dostęp do rachunku w takiej formie często nazywany jest jako *screen scraping plus*[76].

Wybór rodzaju interfejsu komunikacji z TPP należy do decyzji biznesowej ASPSP, niemniej KNF w swoim komunikacie z dnia 12 stycznia 2018 r.[77] wskazała, że z punktu

[73] Definicja „szczególnie chronionych danych dotyczących płatności" została przedstawiona w rozdziale 4.1.
[74] ASPSP może zaprojektować specjalny interfejs komunikacji z TPP we własnym zakresie lub skorzystać z dostępnych standardów rynkowych, które opisano w rozdziale 6 i 7.
[75] Patrz rozdział 4.9. *Identyfikacja TPP z wykorzystaniem certyfikatów eIDAS*.
[76] Patrz rozdział 4.13. *Ochrona indywidualnych danych uwierzytelniających użytkownika*.
[77] *Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 12 stycznia 2018 r. dotyczący wybranych oczekiwań nadzorczych w odniesieniu do okresu przejściowego związanego z implementacją Dyrektywy PSD2*: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_w_sprawie_PSD2_60678.pdf

widzenia zapewnienia efektywnej kontroli nad zakresem udostępnianych danych bezpieczniejszym rozwiązaniem jest stworzenie specjalnego interfejsu API.

4.6. WYMOGI DLA SPECJALNEGO INTERFEJSU KOMUNIKACJI

a) Poziom dostępności i efektywności interfejsu

Wymogi zawarte w art. 32 ust. 1 RTS wskazują, że wprowadzony przez ASPSP specjalny interfejs komunikacji z TPP powinien stale oferować **ten sam poziom dostępności i efektywności** – **w tym wsparcia** – co interfejsy udostępnione użytkownikowi w celu uzyskania bezpośredniego dostępu do jego rachunku płatniczego w trybie online.

W zakresie powyższego wymogu mogą pojawić się jednak wątpliwości, co oznacza zwrot *ten sam poziom dostępności i efektywności* danego interfejsu[78]. Otóż przepis ten należy interpretować w ten sposób, że **poziom dostępności i efektywności specjalnego interfejsu powinien być co najmniej na tym samym poziomie, jaki jest zapewniany dla interfejsu tradycyjnego**.

b) Wskaźniki efektywności i dostępności interfejsu

ASPSP, który wprowadził specjalny interfejs komunikacji z TPP, zgodnie z art. 32 ust. 2 RTS, jest zobowiązany określić przejrzyste **kluczowe wskaźniki efektywności** (ang. *Key Performance Indicators* – **KPI**) oraz **cele dostępności** (ang. *Service Level Targets* – **SLT**), odnoszące się do: (1) procesu rozwiązywania problemów w funkcjonowaniu interfejsu, (2) wsparcia technicznego poza godzinami pracy ASPSP, (3) monitorowania poziomu KPI i SLT, (4) planów awaryjnych oraz (5) utrzymania rozwiązań zapewniających efektywność specjalnego interfejsu.

Powyższe wskaźniki i cele powinny być przynajmniej **w równym stopniu rygorystyczne** – zarówno pod względem dostępności, jak i przekazywanych danych – co wskaźniki i cele ustalone w odniesieniu do tradycyjnego interfejsu stosowanego przez użytkowników. W przypadku oferowania przez ASPSP kilku interfejsów użytkownika (np. serwis internetowy, mobilny itp.) w celu porównania z API wybiera się interfejs o najwyższym poziomie dostępności i efektywności.

Wytyczne EBA[79] z dnia 4 grudnia 2018 r. (Wytyczna 2) wskazują na wprowadzenie przez ASPSP przynajmniej dwóch **KPI dotyczących dostępności specjalnego interfejsu**[80]:

---

[78] W opinii niektórych uczestników rynku wymóg utrzymywania dwóch interfejsów na takim samym poziomie usług, z technicznego punktu widzenia, może być trudny do spełnienia.

[79] Mowa o *Wytycznych w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji)* (EBA/GL/2018/07) dostępnych na stronie EBA pod adresem: https://eba.europa.eu/documents/10180/2570450/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back_PL.pdf/0580ad7a-3c40-48ef-9d86-71c15245eabc

[80] KPI ustalane są indywidualnie przez ASPSP dla każdego z interfejsów użytkownika.

a) **czasu nieprzerwanej pracy** wszystkich interfejsów w ciągu dnia (procentowa dostępność interfejsów z uwzględnieniem przerw w pracy – przestojów) oraz
b) **czasu przerw w pracy** (okres niedostępności) wszystkich interfejsów w ciągu dnia (łączna liczba sekund, w czasie których specjalny interfejs nie działał w ciągu 24 godzin od północy do północy).

W obliczeniach powyższych wskaźników należy przyjmować, że interfejs nie działa, gdy po **5** kolejnych żądaniach dostępu do informacji w celu świadczenia usług PIS, AIS i CAF nie uzyska się odpowiedzi **w łącznym czasie 30 sekund**, niezależnie od tego, czy żądania te pochodzą od jednego, czy od większej liczby dostawców PIS, AIS lub CAF. W takiej sytuacji ASPSP powinien obliczyć czas przestoju od chwili otrzymania pierwszego z pięciu kolejnych żądań, na które nie udzielono odpowiedzi w ciągu 30 sekund, pod warunkiem że w tych pięciu żądaniach nie było żadnego udanego, na które nastąpiła reakcja.

W zakresie oceny dostępności interfejsów może pojawić się pytanie, w jaki sposób traktować planowane z wyprzedzeniem **cykliczne przerwy serwisowe**. Co do zasady, planowane przerwy będą obniżać poziom dostępności danego interfejsu, gdyż w rezultacie uniemożliwiają TPP i użytkownikom korzystanie z elektronicznych kanałów dostępu do systemów transakcyjnych, których założeniem jest funkcjonowanie w trybie całodobowym. Z drugiej strony planowanych przerw serwisowych nie należy porównywać z nagłymi przerwami wynikającymi z awarii systemów ASPSP. Uznając, że takie planowane przerwy nie byłyby brane pod uwagę przy wyliczeniach wartości wskaźników dostępności interfejsów, wówczas ASPSP powinien z odpowiednim wyprzedzeniem poinformować TPP i użytkowników o planowanej przerwie serwisowej oraz określić maksymalny czas trwania takiej przerwy (wskazać godziny niedostępności danego interfejsu). Należy przy tym podkreślić, że **ASPSP powinien przestrzegać przyjętych zasad organizacji przerw serwisowych i wyliczania wskaźników dostępności interfejsów, gdyż wszelkie niepożądane zachowania ASPSP w tym zakresie będą mogły być przedmiotem wyjaśnień ze strony KNF**.

Oprócz KPI dotyczących dostępności ASPSP powinien wprowadzić przynajmniej następujące **KPI dotyczące działania (efektywności) specjalnego interfejsu**, tj.:
a) średni dzienny czas (w milisekundach) przypadający na jedno żądanie, po którym ASPSP przekazuje dostawcy PIS wszystkie wymagane informacje w celu realizacji transakcji;
b) średni dzienny czas (w milisekundach) przypadający na jedno żądanie, po którym ASPSP przekazuje dostawcy AIS wszystkie wymagane informacje nt. rachunku płatniczego użytkownika;
c) średni dzienny czas (w milisekundach) przypadający na jedno żądanie, po którym ASPSP przekazuje dostawcy CAF potwierdzenie w formie „TAK/NIE" odnośnie dostępności określonej kwoty środków na rachunku płatniczym użytkownika;
d) dzienny wskaźnik reakcji na błąd – obliczony jako liczba komunikatów o błędach dotyczących błędów, które można przypisać ASPSP, wysłanych w ciągu dnia przez tego dostawcę do dostawcy PIS, AIS i CAF, podzielona przez liczbę żądań otrzymanych w tym samym dniu przez ASPSP od dostawcy AIS, PIS i CAF.

Jednocześnie należy wskazać, że wg opinii EBA[81] przy obliczaniu wskaźników przedstawionych powyżej w punktach a–c czas na udzielenie przez ASPSP odpowiedzi na żądanie TPP obejmuje również czas niezbędny do weryfikacji zezwolenia/rejestracji TPP, w tym certyfikatu eIDAS. Ponadto w przypadku usługi PIS (pkt a) czas ten obejmuje także czas potrzebny do przeprowadzenia procedury silnego uwierzytelniania klienta.

c) Publikacja statystyk w zakresie efektywności i dostępności interfejsu

Wymogi art. 32 ust. 4 RTS wskazują, że ASPSP, który wprowadził specjalny interfejs komunikacji z TPP, powinien monitorować jego dostępność i efektywność. Ponadto ASPSP jest zobowiązany publikować na swojej stronie internetowej **kwartalne statystyki** dotyczące dostępności i efektywności specjalnego interfejsu oraz interfejsu tradycyjnego udostępnianego swoim użytkownikom.

Zgodnie z Wytycznymi EBA (Wytyczna 3) ASPSP powinien przekazać do KNF **plan publikacji** kwartalnych statystyk dotyczących dostępności i efektywności specjalnego oraz tradycyjnego interfejsu wraz z informacjami o tym, gdzie statystyki te zostaną opublikowane i kiedy nastąpi ich pierwsza publikacja.

W ocenie UKNF pierwsza data publikacji powyższych statystyk może nastąpić **po upływie pierwszego pełnego kwartału powszechnego stosowania specjalnego interfejsu przez TPP**. Jeżeli został on udostępniony do powszechnego stosowania np. w dniu 14 września 2019 r., wówczas data pierwszej publikacji powinna nastąpić po dniu 1 stycznia 2020 r. Kolejne publikacje powinny następować **po zakończeniu kolejnych pełnych kwartałów powszechnego stosowania interfejsu**. Daty publikacji statystyk zależą więc od daty pierwszego udostępnienia specjalnego interfejsu do powszechnego stosowania przez TPP.

Publikacja statystyk powinna umożliwić TPP oraz użytkownikom usług płatniczych porównanie dostępności i efektywności specjalnego interfejsu z dostępnością i efektywnością każdego z interfejsów tradycyjnych udostępnionych przez ASPSP w ramach bankowości elektronicznej.

d) Testy warunków skrajnych

Ustanowiony przez ASPSP specjalny interfejs komunikacji z TPP, jak również kluczowe wskaźniki efektywności (KPI) i cele w zakresie gwarantowanego poziomu usług (SLT), zgodnie z art. 32 ust.2 RTS, powinny podlegać **monitorowaniu i testom warunków skrajnych** (tzw. stress testom).

Wytyczne EBA wskazują, że na potrzeby przeprowadzenia testów warunków skrajnych ASPSP, zgodnie z Wytyczną 4, powinien opracować **metodologię** (procesy) pozwalającą ustalić i ocenić wpływ warunków skrajnych (np. duża liczba zapytań TPP)

[81] Opinia EBA dotycząca wyliczania wskaźnika czasu odpowiedzi ASPSP na zapytanie TPP została przedstawiona w ramach wyjaśnienia kwestii XXII podnoszonej przez członków Grupy roboczej EBA ds. API: https://eba.europa.eu/documents/10180/2545547/Fifth+set+of+issues+raised+by+EBA+WG+on+APIs.pdf

na dostępność i efektywność specjalnego interfejsu i określonych celów w zakresie gwarantowanego poziomu usług.

Na podstawie przygotowanej metodologii ASPSP powinien przeprowadzić testy specjalnego interfejsu w warunkach skrajnych, obejmujące między innymi następujące działania i funkcje:

a) zdolność zapewnienia dostępu dla wielu dostawców PIS, AIS i CAF;
b) zdolność przetwarzania skrajnie dużej liczby żądań od dostawców PIS, AIS i CAF w krótkim czasie i niezawodnie;
c) użycie skrajnie dużej liczby jednocześnie otwartych sesji w celu inicjowania płatności, uzyskania informacji o rachunku oraz żądania potwierdzenia dostępności środków;
d) żądanie dużych ilości danych.

Dodatkowo, zgodnie z Wytycznymi EBA, ASPSP powinien dostarczyć do KNF **raport** przedstawiający **wyniki testów warunków skrajnych**, w tym założenia przyjęte za podstawę takiego testowania oraz informacje o sposobie rozwiązania każdego z wykrytych problemów.

Jednocześnie w odniesieniu do interpretacji pojęć nieostrych takich jak: *duża liczba żądań*, *duża ilość danych*, w opinii UKNF, ASPSP powinien indywidualnie doprecyzować (zdefiniować) ich zakres, z odpowiednim zastosowaniem zasady proporcjonalności, uwzględniając np. skalę działalności ASPSP oraz obecną skalę usług bankowości internetowej (mierzoną liczbą użytkowników korzystających z tych usług), przyjmując jako punkt odniesienia – tam gdzie jest to możliwe – odpowiednie wartości dla interfejsu, który jest aktualnie bezpośrednio dostępny dla użytkowników bankowości internetowej danego ASPSP. Na poparcie przyjętych założeń ASPSP powinien przedstawić analizy wskazujące, że wartości są rzeczywiście skrajne.

e) Brak przeszkód w świadczeniu usług dostępu do rachunku

Dostęp do rachunku płatniczego użytkownika jest fundamentalnym elementem działalności TPP. Przed uchwaleniem dyrektywy PSD2 odbyło się wiele publicznych debat i konferencji dotyczących tego, czy ASPSP (szczególnie banki) powinny zapewniać TPP dostęp do rachunków swoich użytkowników. Powyższa kwestia została uregulowana w RTS, gdzie każdy ASPSP został zobowiązany udostępnić interfejs komunikacji z TPP na potrzeby świadczenia usług dostępu do rachunku.

Należy przy tym zauważyć, że zgodnie z art. 32 ust. 3 RTS, ASPSP, który wprowadził specjalny interfejs komunikacji z TPP, powinien zapewnić, aby **interfejs ten nie stwarzał przeszkód** (ang. *obstacles*) w świadczeniu usług PIS i AIS. Przeszkody takie mogą obejmować m.in. uniemożliwianie dostawcom PIS i AIS wykorzystywania danych uwierzytelniających wydanych przez ASPSP dla jego użytkowników, wymuszanie przekierowania do mechanizmu uwierzytelniania lub innych funkcji ASPSP, wymóg uzyskania dodatkowych zezwoleń oraz dodatkowych rejestracji oprócz tych

przewidzianych w art. 11, 14 i 15 PSD2[82] lub wymóg dodatkowej weryfikacji zgody udzielonej dostawcom PIS i AIS przez użytkowników usług płatniczych.

Wytyczne EBA wskazują natomiast, że ASPSP w celu wykazania spełnienia powyższego wymogu RTS, zgodnie z Wytyczną 5, powinien przekazać do KNF:

a) opis udostępnionych metod uwierzytelniania użytkownika wykorzystywanych przez specjalny interfejs komunikacji;
b) uzasadnienie, dlaczego w ocenie ASPSP udostępnienie takiej metody lub metod uwierzytelniania użytkownika nie stanowi przeszkody w rozumieniu art. 32 ust. 3 RTS (wraz z potwierdzeniem braku przeszkód do świadczenia usług przez TPP);
c) informację, w jaki sposób udostępniona metoda lub metody uwierzytelniania umożliwiają dostawcy PIS i AIS oparcie się na metodach uwierzytelniania stosowanych przez użytkownika w ramach tradycyjnego interfejsu komunikacji z TPP;
d) opis okoliczności potwierdzających, że interfejs nie powoduje niepotrzebnych opóźnień w korzystaniu przez użytkownika z usług TPP i nie wiąże się z koniecznością podejmowania zbędnych kroków oraz nie wykorzystuje niejasnego lub zniechęcającego języka, co mogłoby pośrednio lub bezpośrednio zniechęcać użytkownika do korzystania z usług TPP.

Jednocześnie należy podkreślić, że wskazanie w RTS przykładowych funkcji specjalnego interfejsu komunikacji, które **mogą** stanowić potencjalne przeszkody w świadczeniu usług dostępu do rachunku, nie oznacza, że funkcji tych nie można stosować w przypadku, gdy ASPSP zapewni TPP sprawny dostęp do rachunków płatniczych użytkowników. Przykładem może być metoda uwierzytelniania użytkownika stosowana w płatnościach internetowych typu *pay-by-link*, zwana potocznie *redirection*, która opiera się na przekierowaniu użytkownika na stronę ASPSP celem bezpośredniego zalogowania się do swojego konta. Powyższa metoda jest jedną z form uwierzytelniania użytkownika określonych w standardzie PolishAPI, który szerzej został opisany w rozdziale 6.

4.7. MECHANIZMY AWARYJNE DLA SPECJALNEGO INTERFEJSU KOMUNIKACJI

W celu zagwarantowania TPP świadczenia usług dostępu do rachunku w oparciu o specjalny interfejs komunikacji, w przypadku wystąpienia problemów związanych z dostępnością lub nieprawidłowym działaniem tego interfejsu, RTS nałożył na ASPSP określone wymogi.

Zgodnie z art. 33 ust.1 RTS projekt specjalnego interfejsu komunikacji z TPP powinien uwzględniać **strategię i plany w zakresie środków awaryjnych** na wypadek, gdyby interfejs nie działał zgodnie z wymogami RTS, bądź na wypadek nieplanowanej

[82] Przepisy art. 11, 14 i 15 PSD2 odnoszą się odpowiednio do wymogu posiadania zezwolenia na prowadzenie działalności w charakterze instytucji płatniczej, wymogu prowadzenia przez państwo członkowskie lokalnego rejestru dostawców usług płatniczych oraz wymogu prowadzenia przez EBA unijnego rejestru dostawców usług płatniczych.

niedostępności interfejsu lub awarii systemów. Przyjmuje się, że nieplanowana niedostępność lub awaria systemów występuje w sytuacji, jeżeli na **5** następujących po sobie żądań dostępu do informacji niezbędnych do świadczenia usług PIS lub AIS nie zostanie udzielona odpowiedź **w ciągu 30 sekund.**

Wskazane powyżej środki awaryjne powinny obejmować plany komunikacji służące poinformowaniu TPP korzystających ze specjalnego interfejsu o środkach mających na celu przywrócenie systemu oraz opis natychmiast dostępnych wariantów alternatywnych, z których TPP mogą w tym czasie skorzystać.

Szczególnym wymogiem nałożonym na ASPSP jest umożliwienie TPP, w ramach przyjętych mechanizmów awaryjnych, korzystania z interfejsu tradycyjnego udostępnionego użytkownikom usług płatniczych na potrzeby uwierzytelniania i komunikacji z ASPSP do momentu przywrócenia poziomu dostępności i efektywności specjalnego interfejsu do poziomu utrzymywanego dla interfejsu tradycyjnego. Jest to tzw. **opcja *fallback***[83].

W ramach opcji *fallback*, ASPSP jest zobowiązany zapewnić TPP możliwość identyfikowania się wobec ASPSP[84] oraz polegania na procedurach uwierzytelniania użytkowników usług płatniczych (w praktyce użytkownik będzie proszony o przekazanie TPP np. loginu i hasła do systemu bankowości elektronicznej)[85].

Jeżeli TPP chce korzystać z interfejsu tradycyjnego w ramach opcji *fallback*, to zgodnie z art. 33 ust. 5 RTS powinien:

a) wprowadzić niezbędne środki w celu zapewnienia, aby nie miał on dostępu do danych, nie przechowywał ani nie przetwarzał ich w celach innych niż świadczenie usług zleconych przez użytkownika;
b) w dalszym ciągu przestrzegać obowiązków wynikających z dyrektywy PSD2[86];
c) rejestrować dane, do których dostęp uzyskano za pośrednictwem interfejsu tradycyjnego, i na wniosek bez zbędnej zwłoki przedstawiać pliki rejestrów do KNF;
d) na wniosek i bez zbędnej zwłoki uzasadnić KNF korzystanie z interfejsu tradycyjnego;
e) odpowiednio informować ASPSP o wszelkich działaniach podejmowanych w związku z dostępem do rachunku użytkownika.

4.8. WYŁĄCZENIE Z OBOWIĄZKU ZAPEWNIENIA OPCJI *FALLBACK*

Wprowadzenie opcji *fallback* w przepisach RTS daje TPP gwarancję ciągłości działania usług dostępu do rachunku, ale może też powodować pewne obawy po stronie ASPSP związane z bezpieczeństwem danych uwierzytelniających użytkowników przechowywanych po stronie TPP.

---

[83] Zwana również mechanizmem rezerwowym (ang. *fallback mechanism*).
[84] Patrz też rozdział 4.9. *Identyfikacja TPP z wykorzystaniem certyfikatów eIDAS*.
[85] Patrz też rozdział 4.13. *Ochrona indywidualnych danych uwierzytelniających użytkownika*.
[86] Dotyczy przestrzegania wymogów dyrektywy PSD2 wynikających z art. 66 ust. 3 (obowiązki dostawcy PIS) i art. 67 ust. 2 (obowiązki dostawcy AIS).

Biorąc pod uwagę powyższe, zgodnie z art. 33 ust. 6 RTS, KNF – po przeprowadzeniu konsultacji z EBA[87] – może objąć wyłączeniem z obowiązku zapewnienia opcji *fallback* tych ASPSP, którzy zdecydowali się na wprowadzenie specjalnego interfejsu, jeżeli interfejs ten spełnia **4** poniższe warunki:

1) jest dostosowany do wymogów wynikających z RTS[88],
2) został opracowany i przetestowany w sposób zadowalający TPP[89],
3) od co najmniej 3 miesięcy jest dostępny i powszechnie stosowany przez TPP,
4) wszelkie problemy związane ze specjalnym interfejsem rozwiązano bez zbędnej zwłoki.

Szczegółowe zasady stosowania art. 33 ust. 6 RTS zarówno przez KNF, jak i dostawców usług płatniczych zostały określone w Wytycznych EBA.

Poniżej opisano warunki uzyskania zwolnienia z opcji *fallback*, które ASPSP powinien uwzględnić podczas składania stosownego wniosku do KNF.

Opracowanie i przetestowanie interfejsu w sposób zadowalający TPP

ASPSP w celu udokumentowania zgodności z wymogiem RTS dotyczącym opracowania specjalnego interfejsu w sposób zadowalający TPP, zgodnie z Wytycznymi EBA (Wytyczna 6), powinien przekazać do KNF:

a) dowód na to, że specjalny interfejs spełnia wymogi prawne dotyczące dostępu i danych ujęte w dyrektywie PSD2 i RTS, w tym:
   - opis rozwiązań funkcjonalnych i technicznych zastosowanych przez ASPSP (w przypadku implementacji standardu rynkowego należy wskazać, która norma inicjatywy rynku[90] jest wdrażana przez ASPSP, niezależnie od tego, czy odbiega on w jakimś konkretnym aspekcie od takiej normy, a jeśli tak, to pod jakim względem odbiega od takiej normy i w jaki sposób spełnia wymogi PSD2 i RTS);
   - podsumowanie, w którym opisano, w jaki sposób wdrożenie tych rozwiązań spełnia wymogi PSD2 i RTS (w przypadku implementacji standardu rynkowego należy przekazać, gdy są dostępne, wyniki testów zgodności opracowanych w ramach inicjatywy rynku, które potwierdzają zgodność interfejsu z odpowiednią normą przyjętą przez inicjatywę rynku);
b) informacje o tym, czy – a jeśli tak, to w jaki sposób – ASPSP nawiązał współpracę z TPP.

Wytyczne EBA nie precyzują zakresu informacji, jakie ASPSP powinien przedstawić organowi nadzoru w celu przedstawienia opisu działań podejmowanych wspólnie

---

[87] Wytyczne EBA (Wytyczna 9.1.) wskazują, że udzielenie przez KNF zezwolenia na wyłączenie z opcji *fallback* nie może nastąpić przed otrzymaniem opinii EBA lub przed upływem miesiąca od notyfikacji przez KNF zamiaru udzielenia takiego zezwolenia.

[88] Określonych w art. 32 RTS.

[89] Patrz rozdział 4.4. *Środowisko testowe dla interfejsu komunikacji*.

[90] Inicjatywa rynku oznacza grupę interesariuszy, którzy opracowali specyfikację techniczną dla specjalnego interfejsu komunikacji, prowadząc jednocześnie konsultacje z TPP.

z TPP w ramach podjętej współpracy, która ma prowadzić do opracowania specyfikacji technicznej dla specjalnego interfejsu.

W ocenie UKNF w przypadku gdy wprowadzony przez ASPSP interfejs komunikacji opiera się na standardzie rynkowym, wystarczające w tym zakresie jest przekazanie ogólnych informacji wskazanych w Wytycznych EBA – pkt b powyżej.

Natomiast w przypadku gdy specjalny interfejs rynkowy nie będzie opierać się na żadnym standardzie rynkowym, w opinii UKNF, ASPSP powinien przekazać KNF dodatkowe informacje, obejmujące:

a) datę rozpoczęcia i zakończenia współpracy ASPSP z TPP w zakresie opracowania specyfikacji technicznej dla specjalnego interfejsu, w tym liczbę TPP[91], którzy (aktywnie lub pasywnie) brali udział w prowadzonych pracach z podziałem na dostawców PIS, AIS i CAF;
b) skrócony opis charakteru współpracy ASPSP z TPP, w tym:
   - wskazanie częstotliwości organizowanych spotkań lub telekonferencji;
   - ogólną informację o kwalifikacjach zespołu wyznaczonego w ASPSP, który był odpowiedzialny za organizację takiej współpracy i prac rozwojowych nad interfejsem (liczba osób wchodzących w skład zespołu, kwalifikacje zawodowe);
   - informacje o prowadzonych konsultacjach umożliwiających zgłaszanie przez TPP uwag i zastrzeżeń co do sposobu zaprojektowania lub funkcjonowania specjalnego interfejsu;
   - ogólny opis sposobu, w jaki ASPSP dokonywał oceny zasadności uwag lub zastrzeżeń zgłaszanych przez TPP;
c) dodatkowe informacje dotyczące zasad organizacji współpracy z TPP, które ASPSP uzna za istotne.

W związku z wymogiem RTS dotyczącym testowania specjalnego interfejsu komunikacji ASPSP powinien udostępnić **specyfikację techniczną** tego interfejsu upoważnionym TPP lub dostawcom usług płatniczych, którzy wystąpili do KNF o stosowne zezwolenie/rejestrację, w tym przynajmniej publikując streszczenie (podsumowanie) specyfikacji specjalnego interfejsu na swojej stronie internetowej[92].

Ośrodek prowadzący testy powinien umożliwić ASPSP, upoważnionym TPP lub dostawcom usług płatniczych, którzy wystąpili do KNF o stosowne zezwolenie/rejestrację przetestowanie specjalnego interfejsu w bezpiecznym, specjalnym środowisku testowym z wykorzystaniem danych testowych użytkowników pod kątem:

a) stabilności i bezpieczeństwa nawiązanego połączenia;
b) zdolności ASPSP oraz upoważnionych TPP do wymiany wymaganych certyfikatów eIDAS;
c) zdolności do wysyłania i otrzymywania powiadomień o błędach;

[91] Jeżeli nie jest możliwe wskazanie precyzyjnych danych należy wskazać liczbę orientacyjną.
[92] Patrz rozdział 4.3. *Specyfikacja techniczna dla interfejsu komunikacji.*

d) zdolności dostawcy PIS do wysyłania, a ASPSP – do otrzymywania zleceń inicjowania płatności oraz zdolności ASPSP do udzielania informacji żądanych zgodnie z PSD2/RTS[93];
e) zdolności dostawcy AIS do wysyłania, a ASPSP – do otrzymywania żądań dostępu do danych o rachunku płatniczym oraz zdolności ASPSP do udzielania żądanych informacji[94];
f) zdolności dostawcy CAF do wysyłania, a ASPSP – do otrzymywania żądań od dostawcy CAF oraz zdolności ASPSP do wysyłania do dostawcy CAF potwierdzenia w formie „TAK/NIE" o dostępności środków na rachunku[95];
g) możliwości polegania przez dostawców PIS i AIS na wszystkich procedurach uwierzytelniania zapewnionych przez ASPSP swoim użytkownikom.

EBA wskazuje również, że ASPSP powinien dostarczyć do KNF **podsumowanie wyników testów** dotyczące każdego z elementów poddawanych testom zgodnie z powyższą listą (punkty a-g), w tym liczbę dostawców PIS, AIS i CAF, którzy wykorzystali środowisko testowe, informacje zwrotne otrzymane przez ASPSP od tych dostawców, wykryte problemy oraz opis, w jaki sposób je rozwiązywano.

Powszechne stosowanie interfejsu

Wytyczne EBA wskazują, że w celu udokumentowania spełnienia wymogu RTS dotyczącego powszechnego stosowania interfejsu przez co najmniej 3 miesiące ASPSP, zgodnie z Wytyczną 7, powinien przedstawić organowi nadzoru:
a) opis użycia specjalnego interfejsu przez okres **3 miesięcy** obejmujący między innymi następujące dane:
   - liczbę dostawców PIS, AIS i CAF, którzy wykorzystali interfejs, aby świadczyć usługi użytkownikom, oraz
   - liczbę żądań przesłanych przez powyższych dostawców PIS, AIS i CAF do ASPSP za pośrednictwem specjalnego interfejsu, na które ASPSP zareagował;
b) dowód, że ASPSP podjął wszelkie uzasadnione starania, aby zapewnić powszechne stosowanie swojego specjalnego interfejsu, m.in. poprzez informowanie o jego dostępności za pośrednictwem odpowiednich kanałów, w tym, w stosownych przypadkach, strony internetowej ASPSP, mediów społecznościowych, organizacji branżowych, konferencji oraz bezpośredniej współpracy ze znanymi podmiotami rynku.

EBA ponadto wskazuje, że 3-miesięczny okres stosowania interfejsu może biec jednocześnie z okresem prowadzenia testów, o których mowa w art. 30 ust. 5 RTS[96].

W ocenie UKNF przytoczony powyżej 3-miesięczny okres stosowania interfejsu powinien dotyczyć **fazy produkcyjnej** (mimo możliwości równoległego prowadzenia w tym okresie testów przez TPP), czyli okresu, w którym interfejs jest w pełni

[93] Zgodnie z art. 66 ust. 4 lit. b) PSD 2 oraz art. 36 ust. 1 lit. b) RTS.
[94] Zgodnie z art. 36 ust. 1 lit. a) RTS.
[95] Zgodnie z art. 36 ust. 1 lit. c) RTS.
[96] Patrz rozdział 4.4. *Środowisko testowe dla interfejsu komunikacji*.

wykorzystywany przez TPP na potrzeby świadczenia usług dostępu do rachunku. Jednocześnie należy zaznaczyć, że UKNF jest świadomy tego, że ASPSP w początkowej fazie rozwoju otwartej bankowości, w celu potwierdzenia powszechnego stosowania interfejsu, może spotkać się z problemem braku dostatecznej aktywności TPP na krajowym rynku. W takiej sytuacji organ nadzoru będzie brał pod uwagę całokształt działań podejmowanych przez ASPSP, które miały na celu zachęcić TPP do korzystania z udostępnionego interfejsu.

Niezwłoczne rozwiązywanie problemów związanych z interfejsem

W zakresie udokumentowania spełniania wymogu RTS dotyczącego niezwłocznego rozwiązywania problemów związanych ze specjalnym interfejsem Wytyczne EBA wskazują, że ASPSP, zgodnie z Wytyczną 8, powinien przedstawić KNF:

a) informacje o systemach lub procedurach stosowanych do wykrywania, rozwiązywania i usuwania problemów, szczególnie tych zgłaszanych przez dostawców PIS, AIS i CAF, oraz
b) wyjaśnienie problemów, szczególnie tych zgłaszanych przez dostawców PIS, AIS i CAF, których nie rozwiązano zgodnie z określonymi przez ASPSP celami w zakresie gwarantowanego poziomu usług.

Warunki procedowania wniosku o zwolnienie z opcji fallback

UKNF w swoim komunikacie[97] z dnia 1 lipca 2019 r. wskazał, że zwolnienie przez KNF z opcji *fallback* powinno następować **w drodze decyzji administracyjnej** wydanej indywidualnie dla każdego podmiotu po przeprowadzeniu postępowania administracyjnego, na wniosek zainteresowanego ASPSP, spełniającego wymogi art. 33 ust. 6 RTS.

Ponadto w powyższym komunikacie UKNF poinformował, że wszystkie wnioski KNF będzie rozpatrywała odrębnie dla każdego ASPSP. Jednocześnie nadzór wskazał, że sprawdzenie, czy dany ASPSP spełnia warunki zwolnienia czy nie, może odbywać się w ramach bieżącego nadzoru, jeszcze przed przygotowaniem i dostarczeniem do KNF wniosku przez zainteresowane instytucje.

Podkreślić należy, że nawet w przypadku ostatecznego zwolnienia ASPSP z opcji *fallback* ryzyko związane z choćby przejściowym niewypełnieniem obowiązku jej posiadania po 13 września 2019 r. i w związku z tym uniemożliwieniem TPP świadczenia jego usług obciąża obowiązany ASPSP.

Jednocześnie należy pamiętać, że zgodnie z art. 33 ust. 7 **KNF może cofnąć wyłączenie** z obowiązku ustanowienia opcji *fallback*, jeżeli ASPSP nie spełnia warunków określonych w RTS przez okres dłuższy niż **2 następujące po sobie tygodnie**

[97] *Komunikat Urzędu Komisji Nadzoru Finansowego w sprawie zwolnienia z tzw. opcji fallback* z dnia 1 lipca 2019 r. dostępny pod adresem: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_Urzedu_KNF_w_sprawie_zwolnienia_z_tzw_opcji_fallback.pdf

kalendarzowe. KNF przekazuje do EBA informację o cofnięciu wyłączenia i zapewnia, aby ASPSP ustanowił opcję *fallback* w najkrótszym możliwym terminie, a najpóźniej **w ciągu 2 miesięcy**.

Oczekiwania KNF w przypadku korzystania z opcji fallback

W komunikacie UKNF z dnia 1 lipca 2019 r.[98] wskazano, że ASPSP, który nie będzie zainteresowany zwolnieniem z opcji *fallback* lub nie będzie w stanie spełnić wymogów dla takiego zwolnienia, powinien utworzyć, wdrożyć i utrzymywać mechanizm awaryjny. RTS wymaga, aby w ramach opcji *fallback* ASPSP umożliwiał TPP korzystanie z interfejsów udostępnionych użytkownikom na potrzeby uwierzytelniania i komunikacji z ASPSP. Takie sformułowanie wskazuje, że w przypadku zastosowania opcji *fallback* TPP może uzyskać dostęp do danych identyfikujących i uwierzytelniających użytkownika (login, hasło) na potrzeby komunikacji elektronicznej z ASPSP. Stosowanie opcji *fallback*, w opinii KNF, powinno w związku z tym uwzględniać w szczególności następujące zasady:

- ✓ zapewnienie, aby TPP korzystający z opcji *fallback* był należycie zidentyfikowany i uwierzytelniony stosownym certyfikatem elektronicznym[99];
- ✓ dostęp TPP do danych użytkownika i informacji o jego produktach przy zastosowaniu opcji *fallback* powinien być taki sam jak w przypadku normalnej komunikacji poprzez specjalny interfejs (API);
- ✓ jeżeli w wyniku zastosowania opcji *fallback* doszło do ujawnienia jakimkolwiek podmiotom trzecim, w tym TPP, indywidualnych danych uwierzytelniających użytkownika (np. wielorazowego hasła dostępowego), dane te należy traktować jako skompromitowane – stosownie do odpowiednich procedur ASPSP dotyczących bezpieczeństwa (następstwem tego powinno być w szczególności wymuszenie zmiany tych danych przy próbie następnego logowania przez użytkownika oraz przekazanie użytkownikowi niezbędnych informacji i wyjaśnień);
- ✓ ASPSP powinien oceniać i monitorować ryzyko ujawniania indywidualnych danych uwierzytelniających użytkownika podmiotom trzecim. Jeżeli w szczególności na podstawie liczby zapytań kierowanych przez TPP do API, analizy awaryjności API lub częstotliwości stosowania opcji *fallback* ryzyko to jest oceniane jako wysokie, ASPSP powinien dążyć do jego ograniczenia, w szczególności poprzez wdrażanie rozwiązań w zakresie mechanizmów awaryjnych, wyłączających możliwość ujawniania indywidualnych danych uwierzytelniających użytkownika.

4.9. IDENTYFIKACJA TPP Z WYKORZYSTANIEM CERTYFIKATÓW eIDAS

Istotnym wymogiem wynikającym z RTS jest obowiązek identyfikowania się TPP względem ASPSP podczas świadczenia usług dostępu do rachunku. Zagadnienie to jest istotne z punktu widzenia bezpieczeństwa danych użytkowników. W praktyce TPP, który nawiązuje połączenie z ASPSP za pośrednictwem ustanowionego

[98] Ibidem.

[99] Patrz rozdział 4.9. *Identyfikacja TPP z wykorzystaniem certyfikatów eIDAS*.

interfejsu komunikacji, powinien przedstawić się jako zaufana strona trzecia i potwierdzić uprawnienia do wykonywania określonych usług.

Zgodnie z art. 34 ust. 1 RTS, TPP do celów identyfikacji wobec ASPSP powinien wykorzystywać tzw. **certyfikaty eIDAS**, tj.:
1) **kwalifikowane certyfikaty pieczęci elektronicznych** (ang. *Qualified Certificates for Electronic Seals – QSealC*) lub
2) **kwalifikowane certyfikaty uwierzytelniania witryn internetowych** (ang. *Qualified Certificates for Website Authentication* – QWAC),

o których mowa w *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE* (zwanym dalej: rozporządzeniem eIDAS[100]).

Certyfikaty eIDAS wykorzystywane przez dostawców TPP mogą być wydawane jedynie przez **kwalifikowanych dostawców usług zaufania** (ang. *Qualified Trust Service Providers* – QTPS) spełniających wymagania rozporządzenia eIDAS w odniesieniu do notyfikowanych systemów identyfikacji elektronicznej[101]. W Polsce podmioty takie wpisane są do rejestru **Narodowego Centrum Certyfikacji** (NCCert) prowadzonego przez Narodowy Bank Polski[102].

RTS wprowadza pewne **dodatkowe wymogi w odniesieniu do zawartości certyfikatów eIDAS** stosowanych na potrzeby usług dostępu do rachunku, takie jak wskazanie roli dostawcy usług płatniczych wg dyrektywy PSD2 (PISP, AISP, CBPII, ASPSP), organu rejestrującego TPP, numeru rejestracji (zezwolenia) i terminu ważności certyfikatu. Jednocześnie zawarcie tych informacji w ramach certyfikatów eIDAS nie może wpływać na ich interoperacyjność i powszechne uznawanie.

W dniu 11 grudnia 2018 r. EBA wydała opinię[103] w zakresie stosowania certyfikatów eIDAS w związku z RTS. W przedmiotowej opinii EBA odnosi się w szczególności do pytań zgłaszanych przez uczestników rynku związanych ze stosowaniem kwalifikowanych certyfikatów pieczęci elektronicznych, które, w odróżnieniu od kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, nie posiadają odpowiednich zabezpieczeń kryptograficznych gwarantujących poufność przekazywanych danych. Z drugiej strony pieczęcie mogą stanowić dowód dla stron trzecich (np. klientów)

[100] W Polsce obowiązuje również *Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej* (Dz. U. z 2019 r. poz. 162 t.j. z późn. zm.), która wprowadziła odpowiednie rozwiązania prawne i organizacyjne w celu stosowania rozporządzenia eIDAS.

[101] Certyfikaty eIDAS powinny spełniać wszystkie wymagania specyfikacji technicznej ETSI (TS 119 495) wydanej w 2018 r., która odnosi się do profilu certyfikatów kwalifikowanych na potrzeby PSD2 (*Electronic Signatures and Infrastruktures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and Trusted Services Provider Policy Requirements under PSD2*). Dokument w wersji 1.1.2 dostępny jest adresem: https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.02_60/ts_119495v010102p.pdf

[102] Rejestr Narodowego Centrum Certyfikacji dostępny jest pod adresem: https://www.nccert.pl/uslugi.htm

[103] *Opinion of the European Banking Authority on the use of EIDAS certificates under the RTS on SCA and CSC* (EBA-Op-2018-7): https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf

na autentyczność i integralność danych wykorzystanych do komunikacji, co nie jest możliwe w przypadku certyfikatów witryn internetowych.

Biorąc pod uwagę powyższe, EBA proponuje **3 możliwe sposoby wykorzystywania certyfikatów eIDAS** na potrzeby spełnienia wymogów RTS:

a) jednoczesne stosowanie certyfikowanych pieczęci i witryn internetowych (rozwiązanie pozwala na identyfikację TPP względem ASPSP, zapewnia bezpieczną komunikację i daje gwarancję, że dane pochodzą od dostawcy usług płatniczych wskazanego w certyfikacie);
b) wykorzystywanie wyłącznie certyfikowanych witryn internetowych (rozwiązanie pozwala na identyfikację TPP względem ASPSP, ale nie daje gwarancji, że dane pochodzą od dostawcy usług płatniczych wskazanego w certyfikacie);
c) wykorzystywanie pieczęci elektronicznej z dodatkowymi elementami zapewniającymi bezpieczną komunikację i poufność przekazywanych danych.

Zgodnie z opinią EBA, ASPSP jako strona zapewniająca interfejs komunikacji może sam decydować, jakie certyfikaty eIDAS będzie wykorzystywał na potrzeby spełnienia wymogów RTS, tym niemniej EBA ze względów bezpieczeństwa rekomenduje wybór opcji pierwszej, polegającej na **jednoczesnym stosowaniu certyfikowanych pieczęci i witryn internetowych**. Wybór tej opcji wymaga utworzenia w interfejsie ASPSP odpowiednich funkcjonalności, które umożliwią identyfikację TPP przy użyciu kwalifikowanych pieczęci i witryn internetowych. Takie funkcjonalności powinny zostać zaimplementowane zarówno w specjalnym interfejsie, jak i w ramach dostępu awaryjnego w ramach opcji *fallback*.

Ponadto w opinii EBA wskazano, że jeżeli TPP korzysta z usług np. agentów, dystrybutorów lub prowadzi działalność poprzez oddział, to pożądanym jest **stosowanie wielu certyfikatów**, tj. oddzielnie dla każdego rodzaju podmiotu, w tym podwykonawcy w ramach outsourcingu. W takiej sytuacji ASPSP nie ma prawa odmówić dostępu do rachunku, o ile jest możliwe zidentyfikowanie konkretnego TPP, na rzecz którego działa dany podmiot. W ocenie EBA to TPP odpowiada za działania swoich agentów i dystrybutorów, w tym także za aktualność i poprawność przekazywanych im certyfikatów eIDAS, które identyfikują TPP i dodatkowo zawierają informację o danym agencie. W praktyce ASPSP będzie sprawdzał tożsamość TPP, a nie samego agenta, choć na pewno taki fakt powinien zostać odpowiednio odnotowany. Jednocześnie należy wskazać, że na agentach i dystrybutorach ciąży obowiązek informowania klientów TPP o statusie, który im przyznano, i w imieniu kogo świadczą usługę. ASPSP nie powinien natomiast żądać od nich przedstawienia dodatkowych informacji, jeżeli poprawnie zidentyfikowali się oni z użyciem certyfikatu eIDAS i widnieją w stosownym rejestrze jako agent danego TPP.

Jednocześnie EBA w wydanej opinii[104] zarekomendowała krajowym nadzorcom wprowadzenie odpowiednich rozwiązań w zakresie **weryfikacji aktualności certyfikatów eIDAS**, co ma szczególne znaczenie w kontekście przyznawania, zawieszania

[104] Ibidem.

i cofania zezwoleń/rejestracji na świadczenie usług płatniczych. EBA zaproponowała, aby w przypadku gdy organ nadzoru przykładowo cofnie danemu TPP zezwolenie/zgodę na świadczenie określonych usług płatniczych i nie zostanie poinformowany o unieważnieniu certyfikatu eIDAS ze strony TPP lub kwalifikowanego dostawcy usług zaufania, mógł on wystąpić z wnioskiem do tego dostawcy o unieważnienie certyfikatu, który został przez niego wydany.

Należy dodatkowo wskazać, że status TPP może być weryfikowany przez ASPSP oraz kwalifikowanych dostawców usług zaufania zarówno w lokalnym rejestrze organu nadzoru, jak również w rejestrze stworzonym na poziomie unijnym. W dniu 18 marca 2019 r. **EBA uruchomiła centralny rejestr elektroniczny związany z PSD2** (ang. *Register of payment and electronic money institutions under PSD2*), który zawiera informacje dotyczące m.in.: zarejestrowanych instytucji płatniczych (w tym dostawców PIS), dostawców AIS, instytucji pieniądza elektronicznego oraz agentów oferujących usługi płatnicze na terenie Unii Europejskiej.

Rejestr EBA dostępny jest na stronie internetowej europejskiego urzędu[105], gdzie może być przeglądany za pośrednictwem wyszukiwarki. Możliwe jest również pobranie całej bazy danych zawartych w rejestrze w formacie dostosowanym do jego komputerowej analizy. Informacje zawarte w rejestrze są dostarczane przez krajowe organy nadzorcze, odzwierciedlają treść ich ewidencji i powinny być przez nich aktualizowane **co najmniej raz dziennie**. Na stronie EBA można znaleźć także linki do stron krajowych nadzorów. W przypadku Polski EBA przekierowuje do **Rejestru Usług Płatniczych na stronie internetowej KNF**[106].

Publikacja centralnego rejestru EBA ma na celu zwiększenie transparentności rynku i ochrony użytkowników usług płatniczych. **Rejestr EBA dostępny jest bezpłatnie**, a podmioty można w nim wyszukiwać po nazwie, kraju pochodzenia, numerze identyfikacyjnym czy typie instytucji.

Biorąc pod uwagę wymogi RTS, **rejestr elektroniczny EBA wydaje się niezbędnym narzędziem dla ASPSP na potrzeby funkcjonowania otwartej bankowości**. Pozwala on w szczególności sprawdzić autentyczność i tożsamość TPP, ustalić, czy dany podmiot posiada zezwolenie/rejestrację na prowadzenie działalności i gdzie funkcjonuje w ramach tzw. jednolitego paszportu europejskiego. Należy przy tym wskazać, że prawidłowa identyfikacja TPP zapewnia bezpieczeństwo wszystkim stronom transakcji. ASPSP musi mieć pewność, że nawiązuje kontakt z właściwym podmiotem upoważnionym do świadczenia usług dostępu do rachunku.

[105] https://eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2

[106] https://erup.knf.gov.pl/View/

4.10. BEZPIECZEŃSTWO SESJI KOMUNIKACYJNEJ

Zgodnie z art. 35 RTS, ASPSP oraz TPP powinni stosować **bezpieczne szyfrowanie danych** przez cały czas trwania odpowiednich sesji komunikacyjnych w celu zabezpieczenia poufności i integralności przesyłanych danych, wykorzystując do tego silne i powszechnie uznawane techniki szyfrowania.

Ponadto TPP powinny dążyć do tego, aby zapewniane przez ASPSP sesje dostępu do rachunku użytkownika były możliwie jak najkrótsze, a także czynnie kończyć wszelkie sesje tego rodzaju, gdy tylko żądana czynność została zakończona.

W przypadku utrzymywania równoległych sesji sieciowych z ASPSP dostawcy PIS i AIS powinni zapewnić bezpieczne powiązanie tych sesji z odpowiednimi sesjami ustanowionymi z użytkownikiem lub użytkownikami usług płatniczych, aby zapobiec możliwości nieprawidłowego przekierowania jakiejkolwiek wymienianej między nimi wiadomości bądź informacji. Istotne jest również stosowanie niepowtarzalnej identyfikacji dla inicjowanych transakcji w ramach usługi PIS, żądań użytkowników w ramach usługi AIS oraz żądań związanych z kwotą niezbędną do dokonania transakcji płatniczej w ramach usługi CAF.

Dodatkowo ASPSP oraz dostawcy PIS i AIS podczas przekazywania indywidualnych danych uwierzytelniających użytkowników i kodów uwierzytelniających powinni zapewnić **brak bezpośredniej lub pośredniej możliwości odczytu tych danych przez kogokolwiek z personelu w którymkolwiek momencie.** W przypadku utraty poufności indywidualnych danych uwierzytelniających wchodzących w zakres ich kompetencji, dostawcy ci bez zbędnej zwłoki zobowiązani są **poinformować** o tym użytkownika powiązanego z tymi danymi oraz wydawcę tych indywidualnych danych uwierzytelniających.

4.11. WYMIANA DANYCH Z TPP

Przepisy RTS wprowadzają wymogi dla ASPSP dotyczące zakresu danych udostępnianych TPP. Zgodnie z art. 36 ust. 1 RTS ASPSP powinien:

a) przekazywać dostawcom AIS **te same informacje na temat wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych**, które udostępnia użytkownikowi, gdy ten bezpośrednio żąda dostępu do informacji o rachunku, pod warunkiem, że informacje te nie zawierają szczególnie chronionych danych dotyczących płatności[107];
b) bezzwłocznie po otrzymaniu zlecenia płatniczego udostępniać dostawcom PIS **te same informacje na temat inicjowania i przeprowadzenia transakcji płatniczej**, które przekazuje lub udostępnia użytkownikowi usług płatniczych, gdy ten bezpośrednio zainicjuje transakcję;

[107] Definicja „szczególnie chronionych danych dotyczących płatności" została przedstawiona w rozdziale 4.1.

c) na wniosek bezzwłocznie przekazywać dostawcom CAF **potwierdzenie dostępności na rachunku płatniczym płatnika kwoty** koniecznej do przeprowadzenia transakcji płatniczej w prostym formacie „TAK" lub „NIE".

Odmowa dostępu do rachunku

Na podstawie przepisów PSD2/UUP[108] ASPSP może odmówić dostawcy PIS i AIS dostępu do danego rachunku płatniczego **z obiektywnie uzasadnionych i należycie udokumentowanych przyczyn** związanych z nieuprawnionym lub nielegalnym dostępem do rachunku płatniczego przez takiego dostawcę, w tym nieuprawnionym zainicjowaniem transakcji płatniczej[109]. W takim przypadku ASPSP, w uzgodniony sposób, informuje płatnika o odmowie dostępu do rachunku płatniczego i jej przyczynach. Informacja ta, o ile jest to możliwe, jest przekazywana płatnikowi przed odmową dostępu, a najpóźniej bezzwłocznie po takiej odmowie, nie później jednak niż **w dniu roboczym następującym po dniu takiej odmowy**, chyba że jej przekazanie nie byłoby wskazane z obiektywnie uzasadnionych względów bezpieczeństwa lub jest sprzeczne z odrębnymi przepisami. Jednocześnie ASPSP powinien umożliwić dostawcy PIS i AIS dostęp do rachunku płatniczego niezwłocznie po ustaniu przyczyn uzasadniających odmowę.

4.12. DOPUSZCZALNA CZĘSTOTLIWOŚĆ DOSTĘPU DO INFORMACJI O RACHUNKU

Zgodnie z art. 36 ust. 5 RTS dostawcy AIS mogą uzyskać dostęp do informacji na temat wyznaczonych rachunków płatniczych użytkownika i powiązanych transakcji płatniczych, na potrzeby świadczenia usług AIS, w następujących sytuacjach:

a) zawsze, gdy użytkownik **aktywnie** żąda takich informacji;
b) jeżeli użytkownik nie żąda aktywnie takich informacji, nie więcej niż **4 razy w ciągu 24 godzin**, chyba że – za zgodą użytkownika – dostawca AIS i ASPSP uzgodnią większą częstotliwość.

Powyższe oznacza, że każdy ASPSP powinien na bieżąco monitorować **liczbę żądań** ze strony dostawców AIS w zakresie dostępu do rachunków płatniczych użytkowników i w razie konieczności zwiększyć pojemność/wydajność udostępnionego interfejsu komunikacji, aby zapewnić jego bezawaryjne i sprawne funkcjonowanie.

[108] Art. 41 ust. 5 UUP.
[109] Należy przy tym podkreślić, że w przypadku, gdy odmowa dostępu jest nieuzasadniona, KNF, w drodze decyzji, nakazuje, aby ASPSP bez zbędnej zwłoki przyznał dostawcy PIS lub AIS dostęp do danego rachunku płatniczego.

4.13. OCHRONA INDYWIDUALNYCH DANYCH UWIERZYTELNIAJĄCYCH UŻYTKOWNIKA

Podstawowym elementem zapewnienia bezpieczeństwa użytkowników usług płatniczych jest właściwa ochrona ich indywidulanych danych uwierzytelniających, takich jak np. hasło do systemu bankowości elektronicznej. Zagadnienie to od wielu lat jest istotnym obszarem działań podejmowanych przez ograny regulacyjne i nadzorcze zarówno na poziomie europejskim, jak i krajowym.

Zgodnie z art. 22 RTS dostawcy usług płatniczych zostali zobowiązani zapewnić **poufność i integralność indywidualnych danych uwierzytelniających użytkownika**, w tym również kodów uwierzytelniających, na wszystkich etapach uwierzytelniania. W szczególności RTS wskazuje na obowiązek spełnienia przez dostawców usług płatniczych każdego z określonych poniżej wymogów:

a) indywidualne dane uwierzytelniające są **maskowane** podczas ich wyświetlania i nie można ich w pełni odczytać, kiedy użytkownik wprowadza je podczas uwierzytelniania;
b) indywidualnych danych uwierzytelniających w formacie danych oraz materiałów kryptograficznych powiązanych z szyfrowaniem indywidualnych danych uwierzytelniających nie przechowuje się jako **zwykłego tekstu**;
c) poufny materiał kryptograficzny jest chroniony przed **nieautoryzowanym ujawnieniem**[110].

Dodatkowo dostawcy usług płatniczych powinni zapewnić, aby przetwarzanie i przesyłanie indywidualnych danych uwierzytelniających oraz kodów uwierzytelniających odbywało się w **bezpiecznym środowisku**, zgodnie z niezawodnymi i powszechnie uznanymi standardami branżowymi.

Wymóg określony w art. 23 RTS wskazuje natomiast, aby dostawcy usług płatniczych zapewnili tworzenie indywidualnych danych uwierzytelniających w bezpiecznym środowisku i ograniczyli ryzyko nieuprawnionego wykorzystania tych danych oraz urządzeń uwierzytelniających i oprogramowania uwierzytelniającego w przypadku ich utraty, kradzieży lub skopiowania przed ich dostarczeniem do płatnika.

Niezależnie od powyższego należy wskazać, że przed uchwaleniem dyrektywy PSD2 kwestia ochrony indywidulanych danych uwierzytelniających użytkownika była wielokrotnie podkreślana przez UKNF w związku z praktykowaną wówczas metodą dostępu podmiotów trzecich do rachunków płatniczych zwaną potocznie: ***screen scraping***.

Przed uchwaleniem dyrektywy PSD2 powyższa metoda była w Polsce wykorzystywana głównie przez firmy technologiczne i niektórych dostawców usług płatniczych w celu dostarczania użytkownikom rozwiązań w zakresie płatności internetowych,

[110] Dostawcy usług płatniczych powinni w pełni dokumentować proces związany z zarządzaniem materiałem kryptograficznym wykorzystywanym do szyfrowania indywidualnych danych uwierzytelniających lub uniemożliwiania w inny sposób odczytu tych danych.

informacji o ich saldach na rachunkach w różnych bankach lub w celu przyspieszenia procedury oceny ich zdolności kredytowej. Wykonywanie powyższych usług związane było z koniecznością uzyskania przez takie podmioty dostępu do danych o rachunkach płatniczych użytkowników. **Każda osoba, która chciała skorzystać z tego typu usług, musiała przekazać podmiotowi innemu niż bank dane logowania do swojego konta bankowego, który następnie realizował zleconą usługę, podając się za samego użytkownika**. *Screen scraping* pozwalał zatem stronom trzecim pozyskiwać wiele informacji nt. użytkownika, np. wysokość zarobków, historię wydatków, a pośrednio nawet określać jego preferencje zakupowe i sytuację materialną. **Działania takie mogły prowadzić do naruszeń tajemnicy bankowej, ochrony danych osobowych użytkownika, niechcianego profilowania czy nawet zagrożeń/incydentów związanych z cyberbezpieczeństwem.**

Podejście organu nadzoru do *screen scrapingu*

UKNF w swoim komunikacie z 14 lipca 2014 r.[111] zwrócił uwagę, że podawanie przez użytkowników danych logowania do bankowości internetowej stronom trzecim jest ryzykowne i może prowadzić do **utraty prawa do reklamacji** ewentualnych nieautoryzowanych transakcji ze względu na złamanie przez użytkownika warunków umownych dotyczących korzystania z bankowości internetowej w zakresie konieczności zachowania poufności danych logowania. Dodatkowo organ nadzoru podkreślił, że podstawową zasadą bezpiecznego korzystania z usług bankowych i płatniczych z wykorzystaniem elektronicznych kanałów dostępu jest podawanie nazwy użytkownika i hasła do konta jedynie na stronie internetowej banku prowadzącego dany rachunek lub w udostępnianej przez niego aplikacji (np. instalowanej na smartfonie). UKNF apelował również, że **takie postępowanie może zaprzepaścić wieloletnie działania edukacyjne środowiska bankowego, jak również organu nadzoru** uświadamiające klientom banków istotność powyższej zasady, zaznaczając jednocześnie, że może to spowodować zmniejszenie ich czujności w odniesieniu do miejsc, w których wprowadzają oni swoje dane logowania, powodując tym samym ryzyko stosowania tzw. ***phishingu***[112]. Można sobie bowiem wyobrazić sytuację, w której przestępcy tworzą fałszywą stronę sklepu internetowego, z którego nieświadomy klient, w celu realizacji płatności, zostaje przekierowany na fikcyjną stronę podmiotu trzeciego, gdzie przekazuje swoje dane uwierzytelniające niezbędne do dokonania nielegalnej transakcji.

W wyniku komunikatu UKNF znaczna część dostawców usług płatniczych (w szczególności banków), kierując się względami bezpieczeństwa, podjęła działania mające na celu uniemożliwienie korzystania przez TPP ze *screen scrapingu* i świadczenia usług na bazie tej metody.

---

[111] Komunikat UKNF z dnia 14 lipca 2014 r. pt. *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego*: https://www.knf.gov.pl/knf/pl/komponenty/img/KNF_dane_do_logowania_53315.pdf

[112] *Phishing* – metoda oszustwa polegająca na podszywaniu się pod godną zaufania instytucję (np. bank) w celu wyłudzenia informacji wrażliwych (np. login i hasło do bankowości internetowej, kod autoryzacyjny, dane karty kredytowej) albo nakłonienia ofiary do określonych działań.

Nowe zasady dostępu do rachunku po uchwaleniu dyrektywy PSD2

Uwarunkowania prawne i regulacyjne w zakresie dostępu TPP do rachunku płatniczego użytkownika zmieniły się jednak wraz z przyjęciem dyrektywy PSD2, która ustanowiła zasady świadczenia nowych rodzajów usług, tj. PIS, AIS i CAF. Techniczne zasady świadczenia powyższych usług określone zostały w RTS, które zobowiązały ASPSP do przygotowania interfejsów komunikacji z TPP. Dzięki temu instytucje świadczące nowe rodzaje usług płatniczych, przy spełnieniu określonych wymogów, mogą wejść w posiadanie danych o użytkowniku w zakresie niezbędnym do świadczenia tych usług.

Przepisy RTS wskazują, że ASPSP, w celu zapewnienia TPP dostępu do danych swoich użytkowników, może albo stworzyć specjalny interfejs (API), albo zmodyfikować interfejs już istniejący przewidziany dla uwierzytelniania i komunikacji z własnymi użytkownikami[113]. **Zmodyfikowany interfejs użytkownika musi jednak umożliwiać identyfikowanie się TPP wobec ASPSP z wykorzystaniem certyfikatów eIDAS**[114].

Powyższe oznacza, że od chwili wejścia w życie RTS nie jest możliwe stosowanie dotychczasowej formy *screen scraping*, chociaż nowa wersja tej metody, która na bazie wymogów RTS została przekształcona i rozszerzona o nowe funkcje (obowiązek identyfikowania się TPP wobec ASPSP), określana jest często jako ***screen scraping plus***. W szczególności metoda ta ma uniemożliwić TPP podawanie się za posiadacza rachunku, zadbać o bezpieczeństwo danych użytkownika oraz uchronić go przed niechcianym profilowaniem.

Wybór rodzaju interfejsu komunikacji z TPP należy do decyzji biznesowej ASPSP, niemniej UKNF w swoim komunikacie z 12 stycznia 2018 r.[115] wskazał, że z punktu widzenia zapewnienia efektywnej kontroli nad zakresem udostępnianych danych bezpieczniejszym rozwiązaniem jest **stworzenie specjalnego interfejsu API**. W przypadku gdy ASPSP zdecyduje się na korzystanie z API, TPP, co do zasady, nie będzie mógł żądać dostępu do rachunku w oparciu o metodę *screen scraping plus*. Należy jednak zwrócić uwagę, że zgodnie z art. 33 ust. 4 RTS ASPSP jest zobowiązany zapewnić odpowiedni mechanizm awaryjny (**opcję *fallback***) w przypadku nieplanowanej niedostępności lub awarii ww. interfejsu[116]. ASPSP, w ramach opcji *fallback*, powinien umożliwić TPP – do momentu przywrócenia odpowiedniego poziomu dostępności i efektywności interfejsu API – korzystanie z interfejsu tradycyjnego udostępnionego użytkownikom usług płatniczych na potrzeby uwierzytelniania i komunikacji z ASPSP. W tym przypadku wykorzystywany byłby tradycyjny interfejs oparty na *screen scraping plus*.

---

[113] Patrz rozdział 4.5. *Warianty interfejsu komunikacji*.

[114] Patrz rozdział 4.9. *Identyfikacja TPP z wykorzystaniem certyfikatów eIDAS*.

[115] *Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 12 stycznia 2018 r. dotyczący wybranych oczekiwań nadzorczych w odniesieniu do okresu przejściowego związanego z implementacją Dyrektywy PSD2*: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_w_sprawie_PSD2_60678.pdf

[116] Patrz rozdział 4.7. *Mechanizmy awaryjne dla specjalnego interfejsu komunikacji*.

Z drugiej strony należy zauważyć, że **RTS, pod pewnymi warunkami, umożliwia wyłączenie ASPSP z obowiązku zapewnienia opcji *fallback***. Możliwe jest to po otrzymaniu pozytywnej opinii KNF (konsultowanej wcześniej z EBA) oraz spełnieniu szeregu wymogów dotyczących specjalnego interfejsu API, które obejmują m.in. jego właściwą implementację oraz powszechne stosowanie przez TPP przez okres co najmniej 3 miesięcy[117].

[117] Patrz rozdział 4.8. *Wyłączenie z obowiązku zapewnienia opcji* fallback.

5 RAPORTOWANIE INCYDENTÓW I ZARZĄDZANIE RYZYKIEM WG DYREKTYWY PSD2

Koncepcja otwartej bankowości pozwala kreować różne modele działalności oparte na usługach dostępu do rachunku, ale stawia również przed uczestnikami rynku określone wyzwania związane z zapewnieniem bezpieczeństwa danych oraz środków pieniężnych użytkowników, jak również bieżącym reagowaniem na pojawiające się zagrożenia i ryzyka.

Dyrektywa PSD2 nałożyła na dostawców usług płatniczych, do których można zaliczyć m.in. podmioty funkcjonujące w ramach otwartej bankowości, w szczególności PISP, AISP, CBPII, ASPSP, obowiązek raportowania do organu nadzoru informacji o poważnych incydentach operacyjnych lub poważnych incydentach związanych z bezpieczeństwem.

W dniu 31 października 2018 r. UKNF opublikował komunikat[118], w którym wskazał, że zgodnie z art. 32g UUP **dostawca usług płatniczych powinien niezwłocznie przekazać KNF lub innemu właściwemu organowi nadzoru informację o poważnym incydencie operacyjnym lub incydencie związanym z bezpieczeństwem**, w tym o charakterze teleinformatycznym[119]. Jeżeli incydent ma lub może mieć wpływ na interesy finansowe użytkowników, **dostawca bez zbędnej zwłoki powinien powiadomić o incydencie użytkowników** korzystających z usług tego dostawcy oraz poinformować ich o dostępnych środkach, które mogą podjąć w celu ograniczenia negatywnych skutków incydentu, np. zmiana hasła do systemu bankowości elektronicznej w przypadku wycieku indywidualnych danych uwierzytelniających użytkownika.

Szczegółowe instrukcje dla dostawców usług płatniczych w zakresie zgłaszania incydentów zostały przedstawione w Wytycznych EBA z dnia 19 grudnia 2017 r.[120]

Formularze sprawozdawcze na potrzeby raportowania incydentów wraz z instrukcją ich wypełniania i przesyłania do organu nadzoru dostępne są na stronie internetowej KNF[121].

Jednocześnie należy wskazać, że zgodnie z art. 32f ust.1 UUP dostawca usług płatniczych, w ramach systemu zarządzania ryzykiem, powinien podjąć środki ograniczające ryzyko oraz **wprowadzić mechanizmy kontroli służące zarządzaniu ryzykiem**

---

[118] *Komunikat UKNF z dnia 31 października 2018 r. w sprawie obowiązku raportowania przez dostawców usług płatniczych informacji o incydentach na podstawie PSD2*: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ws_raportowania_incydentow_na_podstawie_PSD2_63638.pdf

[119] Informację o incydencie, KNF lub inny właściwy organ nadzoru przekazują niezwłocznie EBA i ECB, a jeżeli incydent ma znaczenie dla organu nadzoru innego państwa członkowskiego – także temu organowi.

[120] Mowa o *Wytycznych EBA dotyczących poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2)* (EBA/GL/2017/10), dostępnych pod adresem: https://eba.europa.eu/sites/default/documents/files/documents/10180/2066978/5a5de98d-8cbf-4fb4-99ce-67556a129b8b/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10)_PL.pdf

[121] Formularze dostępne są do pobrania pod adresem: https://www.knf.gov.pl/dla_rynku/Informacje_dla_podmiotow_nadzorowanych/Rynek_uslug_platniczych/raportowanie_incydentow_PSD2

operacyjnym oraz ryzykiem naruszenia bezpieczeństwa w zakresie świadczenia usług płatniczych, w szczególności poprzez:

1) **utrzymywanie skutecznej procedury zarządzania incydentami**, w tym na potrzeby wykrywania i klasyfikacji poważnych incydentów operacyjnych i incydentów związanych z bezpieczeństwem, w tym o charakterze teleinformatycznym;
2) **bieżącą ocenę i aktualizację procedur w zakresie zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa**, w tym bezpieczeństwa teleinformatycznego, a także **bieżącą ocenę środków ograniczających ryzyko oraz mechanizmów kontroli.**

Dodatkowo każdy dostawca usług płatniczych corocznie, w terminie **do dnia 31 stycznia roku następnego**, jest zobowiązany przekazać KNF lub innemu właściwemu organowi nadzoru:

a) **roczną informację o ocenie i aktualizacji procedur** w zakresie zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa, a także ocenie środków ograniczających ryzyko oraz mechanizmów kontroli[122];
b) **dane dotyczące oszustw związanych z wykonywanymi usługami płatniczymi**, uwzględniając różne sposoby świadczenia usług płatniczych[123].

Szczegółowe wymogi dla dostawców usług płatniczych w zakresie zarządzania ryzykiem operacyjnym oraz ryzykiem naruszenia bezpieczeństwa w związku ze świadczeniem usług płatniczych określone zostały w Wytycznych EBA z dnia 12 stycznia 2018 r.[124]

[122] Zgodnie z art. 32f ust. 2 UUP.

[123] Zgodnie z art. 32h ust. 1 UUP.

[124] Mowa o *Wytycznych EBA w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (PSD2)* (EBA/GL/2017/17), dostępnych pod adresem: https://eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_PL.pdf/cd60445e-e39b-413a-b297-6a8bedcf7dc2

Jednocześnie należy wskazać, że ww. wytyczne z dniem 30 czerwca 2020 r. zostaną uchylone i zastąpione Wytycznymi EBA z dnia 28 listopada 2019 r. (EBA Guidelines on ICT and security risk management) (EBA/GL/2019/04), dostępnymi pod adresem: https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

6 STANDARD PolishAPI JAKO ISTOTNY ELEMENT OTWARTEJ BANKOWOŚCI

Kluczowym elementem rozwoju otwartej bankowości jest wypracowanie standardów komunikacji umożliwiających współpracę uczestników rynku, w szczególności TPP i ASPSP, za pośrednictwem API.

W 2016 r. Związek Banków Polskich (ZBP), w związku z dyrektywą PSD2, zainicjował prace nad projektem **PolishAPI**, którego celem było stworzenie **wspólnej specyfikacji interfejsu komunikacji z TPP** w oparciu o dostęp do rachunków płatniczych. Uczestnikami inicjatywy standaryzacyjnej PolishAPI są m.in. Związek Banków Polskich wraz ze stowarzyszonymi bankami komercyjnymi i spółdzielczymi, Spółdzielcze Kasy Oszczędnościowo-Kredytowe (SKOK), Polska Organizacja Niebankowych Instytucji Płatności (PONIP) wraz ze stowarzyszonymi firmami, Polska Izba Informatyki i Telekomunikacji (PIIT), Polska Izba Ubezpieczeń (PIU), Krajowa Izba Rozliczeniowa (KIR), Biuro Informacji Kredytowej (BIK), Polski Standard Płatności (PSP)[125].

Podczas prac nad standardem PolishAPI wykorzystywane były dotychczasowe osiągnięcia polskiego sektora bankowego i płatniczego, najlepsze praktyki i doświadczenia, w tym z zagranicznych standardów API, oraz istniejące już interfejsy w ramach infrastruktury międzybankowej.

Standard PolishAPI to istotny element otwartej bankowości na polskim rynku płatniczym obsługiwanym przez banki i podmioty niebankowe. Definiuje interfejs na potrzeby usług świadczonych przez TPP i został stworzony z myślą, by **wspierać rozwój innowacji finansowych (FinTech) w Polsce** w niedyskryminujący i zrównoważony sposób. Inicjatywa budowy lokalnego standardu PolishAPI ma również na celu **obniżenie po stronie uczestników rynku kosztów implementacji wymogów dyrektywy PSD2 i RTS**.

UKNF od samego początku popierał podjętą inicjatywę związaną z budową krajowego standardu PolishAPI. W ocenie organu nadzoru wdrożenie wspólnego standardu w zakresie komunikacji z TPP może zagwarantować **ujednolicone i bezpieczne zasady dostępu** do rachunków płatniczych użytkowników[126].

Pierwsza wersja standardu PolishAPI została oficjalnie opublikowana przez Związek Banków Polskich w dniu 24 kwietnia 2018 r. Twórcy standardu zakładają jego stały rozwój w odpowiedzi na zmiany regulacyjne, technologiczne i biznesowe na rynku

[125] Informacje na temat standardu PolishAPI dostępne są na stronie internetowej: https://polishapi.org. Pełny skład Grupy Projektowej ds. PolishAPI został podany w dokumencie *Specyfikacja interfejsu na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych* na stronach 10–11.
[126] *Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 12 stycznia 2018 r. dotyczący wybranych oczekiwań nadzorczych w odniesieniu do okresu przejściowego związanego z implementacją Dyrektywy PSD2*: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_w_sprawie_PSD2_60678.pdf

polskim oraz europejskim. Kolejne zmiany specyfikacji standardu są publikowane na bieżąco na stronie internetowej PolishAPI.

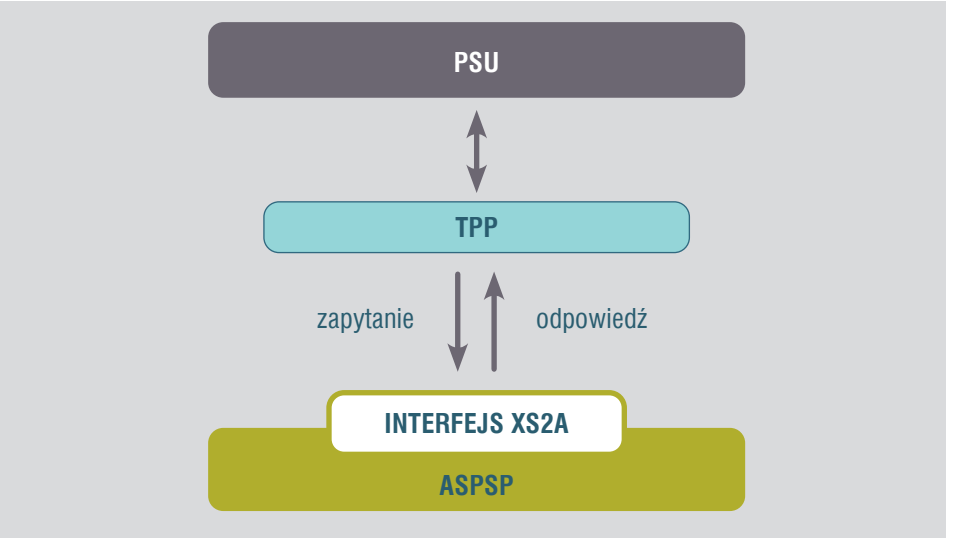
Każdy ASPSP i TPP może skorzystać ze standardu PolishAPI jak z otwartego standardu. Stosowanie standardu nie jest obowiązkowe. Podmioty działające na polskim rynku w oparciu o dyrektywę PSD2 mogą stosować dowolne rozwiązanie, o ile jest ono zgodne pod kątem bezpieczeństwa i funkcjonalności z wymogami prawa, wynikającymi w szczególności z UUP i RTS.

Ogólne założenia standardu

Standard PolishAPI definiuje **3 kategorie aktorów**, którzy mogą wziąć udział w procesach definiowanych w standardzie:

a) *Payment Service User* (PSU) – użytkownik rachunku płatniczego, którego dotyczy dana transakcja płatnicza;
b) *Account Servicing Payment Service Provider* (ASPSP) – dostawca prowadzący rachunek płatniczy i udostępniający interfejs XS2A[127] dla TPP;
c) *Third Party Provider* (TPP) – podmiot korzystający z interfejsu XS2A na podstawie i w ramach zgód wyrażonych przez PSU. ASPSP może występować również jako TPP i korzystać z interfejsów wystawionych przez inne ASPSP.

Ogólny schemat komunikacji w standardzie PolishAPI przedstawiono na rys. 4.



Rys. 4 Ogólny schemat komunikacji w standardzie PolishAPI
Źródło: Specyfikacja standardu PolishAPI

[127] XS2A (ang. *Access to Account*) – dostęp do rachunków płatniczych, wykorzystywany do wykonywania usług AIS, PIS, CAF oraz innych usług realizowanych w ramach standardu PolishAPI.

Zgodnie z powyższym schematem użytkownik usług płatniczych (PSU) może zlecić TPP wykonanie jednej z usług przewidzianych w dyrektywie PSD2, tj. PIS, AIS lub CAF. Następnie TPP, w imieniu i za zgodą użytkownika, nawiązuje kontakt z ASPSP z wykorzystaniem interfejsu XS2A w celu zainicjowania płatności lub pozyskania informacji o rachunku użytkownika.

Komunikacja oparta na standardzie PolishAPI zabezpieczona jest **certyfikatami eIDAS**, wydawanymi przez kwalifikowanych dostawców usług zaufania wg normy standaryzacyjnej TS 119 495[128], zdefiniowanej przez Europejski Instytut Norm Telekomunikacyjnych (ang. *European Telecommunications Standards Institute* – ETSI).

Metody uwierzytelniania użytkownika

Standard PolishAPI definiuje **2 główne metody uwierzytelniania PSU**, których wybór pozostaje wyłącznie w gestii ASPSP:

a) **Metoda *redirection*** – mechanizm uwierzytelniania użytkownika po stronie ASPSP

   Metoda zakłada bezpośrednie przekierowanie PSU na stronę internetową ASPSP podczas realizowania usług AIS, PIS i CAF, co oznacza, że dane uwierzytelniające i autoryzacyjne PSU podawane są **wyłącznie na stronie internetowej ASPSP**. Uwierzytelnienie PSU przeprowadzane jest w interfejsie ASPSP.
   Powyższy sposób znany jest w Polsce z przelewów typu *pay-by-link* realizowanych podczas dokonywania ekspresowych płatności w Internecie, gdzie płatnik jest przekierowywany na stronę swojego banku, na której może podać login i hasło do swojego konta oraz zatwierdzić transakcję.

b) **Metoda *decoupled*** – mechanizm uwierzytelniania użytkownika w zewnętrznym narzędziu autoryzacyjnym

   Metoda umożliwia wykorzystanie mechanizmu uwierzytelniania w zewnętrznym narzędziu autoryzacyjnym podczas realizowania usług AIS i PIS. Mechanizm znany jest z rynków zagranicznych i **polega na skorzystaniu z uwierzytelnienia przeprowadzonego przez niezależny podmiot (zaufaną stronę trzecią) współpracujący z ASPSP**.

[128] TS 119 495 – specyfikacja techniczna normy odnoszącej się do profilu certyfikatów kwalifikowanych na potrzeby dyrektywy PSD2 (*Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU*), opublikowana w 2018 r. Dokument w wersji 1.1.2. dostępny jest pod następującym adresem: https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.02_60/ts_119495v010102p.pdf

W przyszłości w standardzie PolishAPI mogą zostać opisane również **inne mechanizmy uwierzytelniania**[129] spełniające wymogi regulacyjne oraz uzgodnione w ramach prac grupy projektowej, których publikacja nastąpi w kolejnych wersjach specyfikacji.

Przebieg procesu uwierzytelniania użytkownika

Proces uwierzytelniania PSU po stronie ASPSP (metoda *redirection*) lub podmiotu zewnętrznego (metoda *decoupled*) został oparty na **standardzie OAuth 2.0** i prowadzi do wygenerowania **kodu autoryzacyjnego** (ang. *authorization code*) przekazywanego do TPP. W kodzie autoryzacyjnym zawarte są informacje o poprawnym uwierzytelnieniu użytkownika i wyrażeniu przez niego zgody na dostęp TPP do określonych usług i zasobów ASPSP[130].

W dalszej kolejności TPP przekazuje otrzymany kod autoryzacyjny do ASPSP, który generuje tzw. **token dostępu**[131] (ang. *access token*) umożliwiający TPP dostęp do zabezpieczonych zasobów ASPSP za pośrednictwem interfejsu XS2A. W przypadku usługi AIS, ASPSP generuje dodatkowo tzw. *refresh token* umożliwiający TPP pobieranie kolejnych tokenów na potrzeby wielokrotnego pobierania danych o rachunku użytkownika.

Standard PolishAPI definiuje również **zakres informacji** (tabele pól o charakterze obligatoryjnym i fakultatywnym), które ASPSP powinien otrzymać od PSU, za pośrednictwem TPP, w celu umożliwienia realizacji usługi PIS, AIS i CAF.

Rekomendacje Grupy roboczej ds. PolishAPI w zakresie bezpieczeństwa

W dniu 4 września 2019 r. Grupa robocza ds. PolishAPI, działająca przy Związku Banków Polskich, opublikowała dokument *PolishAPI. Rekomendacje dotyczące obszaru bezpieczeństwa dla podmiotów korzystających ze standardu*[132]. Opracowanie składa się z 4 obszarów:
1) Wymagania organizacyjne i procesowe.
2) Wymagania dla infrastruktury systemu.
3) Wymagania dla interfejsu PolishAPI.
4) Przeciwdziałanie nadużyciom i atakom.

Dokument ma zastosowanie do dostawców usług płatniczych wykorzystujących standard PolishAPI, tj. zarówno TPP, jak i ASPSP.

---

[129] Innym znanym na rynku mechanizmem uwierzytelniania użytkownika jest np. metoda *embedded* z wbudowanym wewnętrznym narzędziem autoryzacyjnym.

[130] Zgodnie z PSD2/UUP, TPP może wykonywać usługi na rzecz PSU jedynie za jego zgodą i w zakresie objętym tą zgodą. Standard PolishAPI kompleksowo definiuje ramy udzielania oraz odwoływania zgód PSU na dostęp TPP do określonych usług i zasobów ASPSP.

[131] Token dostępu jest ciągiem znaków, który stanowi techniczną reprezentację sesji komunikacyjnej o ustalonym czasie ważności, nawiązanej pomiędzy TPP i ASPSP w kontekście ściśle określonego PSU i dla ściśle określonego zakresu usług i zasobów po stronie ASPSP, do których TPP uzyskał dostęp.

[132] Dokument w wersji 1.0 dostępny jest na stronie PolishAPI pod następującym adresem: https://polishapi.org/wp-content/uploads/2019/09/PolishAPI-rekomendacja-bezpieczenstwo-v1.0.pdf

Interfejsy PolishAPI udostępnione na polskim rynku

Zgodnie z informacją przedstawioną na stronie PolishAPI na dzień 14 października 2019 r. **środowiska testowe** dla interfejsów komunikacji z TPP oparte na standardzie PolishAPI (wraz z dokumentacją techniczną) udostępniało 18 banków komercyjnych, 516 banków spółdzielczych oraz 7 spółdzielczych kas oszczędnościowo-kredytowych. Jednocześnie należy wskazać, że na dzień 18 listopada 2019 r. dostęp do **środowisk produkcyjnych** zapewniało 14 podmiotów (10 banków komercyjnych, 3 banki spółdzielcze i jedna spółdzielcza kasa oszczędnościowo-kredytowa). Aktualna lista podmiotów udostępniających zarówno środowiska testowe, jak i produkcyjne dla interfejsów komunikacji z TPP dostępna jest na stronie PolishAPI w zakładce *Interfejsy XS2A*[133].

[133] https://polishapi.org/interfejsy-xs2a/

7 INNE UNIJNE INICJATYWY STANDARYZACYJNE NA RZECZ OTWARTEJ BANKOWOŚCI

W związku z dyrektywą PSD2 na terenie Unii Europejskiej powstało kilka wiodących inicjatyw standaryzacyjnych, mających na celu przygotowanie specyfikacji technicznych interfejsów programistycznych (API), udostępnianych przez zobligowane do tego instytucje finansowe, tak aby korzystanie z nich przez TPP było łatwiejsze i bezpieczniejsze.

Do głównych inicjatyw standaryzacyjnych w Unii Europejskiej, oprócz standardu PolishAPI, można zaliczyć[134]:

- ✓ **The Berlin Group NextGenPSD2**[135] – inicjatywa standaryzacyjna o charakterze pan-europejskim, prowadzona przez Grupę Berlińską (ang. *The Berlin Group*) – nieformalną grupę zrzeszającą banki, instytucje i schematy płatnicze, opracowującą standardy rynkowe (m.in. dotyczące rozliczeń kartowych SEPA, płatności mobilnych itp.).

- ✓ **Open Banking UK**[136] – zestaw standardów API dla rynku brytyjskiego, utworzony i zarządzany przez *Open Banking Implementation Entity*, instytucję odpowiedzialną również za opracowanie i prowadzenie katalogu stron trzecich (czyli dostawców usług finansowych, korzystających z dostępu do danych udostępnianych przez banki), zarządzanie reklamacjami oraz nadzór nad implementacją API w brytyjskich bankach.

- ✓ **STET (France)**[137] – standard opracowany przez francuską izbę rozliczeniową (STET), który został w maksymalnym stopniu zbliżony do standardu NextGenPSD2 The Berlin Group, w ramach realizacji projektu konwergencji.

- ✓ **Slovak Banking API**[138] – projekt standaryzacyjny w całości prowadzony przez Związek Banków Słowackich we współpracy z Narodowym Bankiem Słowacji, udostępniany w formie dokumentacji.

W celu implementacji jednolitych standardów API na terenie całej Unii Europejskiej, w styczniu 2018 r., z inicjatywy Komisji Europejskiej, przy Europejskiej Radzie ds. Płatności (EPC) utworzona została **Grupa robocza ds. ewaluacji API** (ang. *API Evaluation Group*) składająca się m.in. z przedstawicieli rynku, w szczególności TPP i ASPSP, stowarzyszeń konsumenckich oraz europejskich organów nadzorczych: EBA i ECB. Założeniem prac Grupy było dokonanie oceny 5 rynkowych inicjatyw standaryzacyjnych (wskazanych powyżej, w tym również standardu PolishAPI) oraz

[134] https://pl.wikipedia.org/wiki/Otwarta_bankowo%C5%9B%C4%87, dostęp z dnia 16.11.2019 r.
[135] https://www.berlin-group.org/psd2-access-to-bank-accounts
[136] https://www.openbanking.org.uk/
[137] https://www.stet.eu/en/psd2
[138] https://sbaonline.docs.apiary.io/#reference

przygotowanie rekomendowanych funkcjonalności API, które byłyby zgodne z wymogami PSD2/RTS[139]. Informacje nt. prowadzonych prac Grupy, które zakończyły się w grudniu 2018 r., dostępne są na stronie EPC[140]. Dalsze prace związane z zagadnieniem implementacji standardów API w świetle wymogów PSD2/RTS kontynuowane są przez **Grupę roboczą EBA ds. API** (ang. *EBA working group on APIs under PSD2*[141]).

[139] https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/api-evaluation-group--recommended-functionalities-psd2rts

[140] https://www.europeanpaymentscouncil.eu/search?kb%5B0%5D=tags%3A4511&node=16301

[141] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2

8 PERSPEKTYWY ROZWOJU OTWARTEJ BANKOWOŚCI W POLSKIM SEKTORZE FINTECH

Sektor podmiotów oferujących usługi finansowe oparte na nowoczesnych technologiach informatycznych (FinTech) rozwija się w Polsce bardzo dynamiczne. Coraz więcej instytucji rynku finansowego (w tym banki) zaczyna traktować innowacyjność jako jedną z głównych metod **budowania przewagi konkurencyjnej**. Zmiany technologiczne pozwalają kreować nowe modele biznesowe, zwiększać zasięg działalności oraz poprawiać jakość świadczonych usług. Konsumenci, w szczególności z młodszych grup wiekowych, pozytywnie przyjmują trend cyfryzacji i chcą korzystać z innowacyjnych rozwiązań, z wykorzystaniem zdalnych kanałów elektronicznych, głównie poprzez sieć Internet oraz urządzenia mobilne.

Do sektora FinTech zalicza się **innowacyjne firmy (często start-upy)** podejmujące działalność regulowaną (lub częściowo regulowaną) na rynku finansowym, jak również **innowacyjne podmioty nadzorowane** (np. banki, instytucje płatnicze) wdrażające nowoczesne rozwiązania technologiczne w zakresie oferowanych produktów lub usług finansowych[142]. Obie kategorie podmiotów nazywane są potocznie fintechami.

Polski sektor bankowy wyróżnia się pod względem technologii na tle Europy. Jest to jedna z najbardziej innowacyjnych polskich branż inwestująca znaczne środki w nowoczesne technologie w takich obszarach, jak np. biometria, sztuczna inteligencja (ang. *artificial intelligence* – AI), w tym uczenie maszynowe (ang. *machine learning* – ML), robotyzacja procesów biznesowych (ang. *Robotic Proces Automation* – RPA), chmura obliczeniowa (ang. *cloud computing*), czy też zdecentralizowane bazy danych oparte na technologii DLT/*blockchain*[143].

Z uwagi na dużą innowacyjność polskiego sektora bankowego **bariera technologiczna pomiędzy firmami technologicznymi a bankami jest w Polsce nieznacząca**. Firmom technologicznym w Polsce w obszarze bankowości i finansów jest dużo trudniej funkcjonować niż na innych rynkach. W polskim sektorze bankowym, ze względu na skalę jego innowacyjności, wiele z tych obszarów, które w zachodniej części Europy są zagospodarowane przez spółki technologiczne, w Polsce są rozwijane przez same banki (np. bankowość mobilna). Oznacza to, że możliwości wprowadzania innowacyjnych usług przez niebankowe fintechy mogą być w Polsce stosunkowo mniejsze niż w innych krajach, w których rozwiązania bankowości elektronicznej nie zostały jeszcze w pełni rozwinięte. Należy jednak pamiętać, że polscy konsumenci są przyjaźnie nastawieni do nowoczesnych usług finansowych i zawsze będzie istniała przestrzeń dla fintechów do oferowania coraz to lepszych rozwiązań, w szczególności zapewniających pozytywne doświadczenia klienta (UX). Wyniki badań przedstawione w raporcie

[142] Na podstawie *Raportu z prac Zespołu roboczego ds. rozwoju innowacji finansowych (FinTech)* (listopad 2017): https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_KNF_11_2017_60290.pdf

[143] DLT (ang. *Distributed Ledger Technology*) – technologia rozproszonych rejestrów, w ramach której można wyróżnić technologię *blockchain*, zwaną inaczej łańcuchem bloków.

KPMG[144] wykazały, że aż **93 proc. Polaków nie ma żadnych problemów w korzystaniu z bankowości elektronicznej**, natomiast kluczem do budowania pozytywnych doświadczeń klientów jest **wiarygodność i personalizacja** przejawiające się zdolnością danej marki do zrozumienia potrzeb klienta i dostarczeniem mu produktów lub usług zgodnych z indywidualnymi oczekiwaniami.

Według sporządzonej przez portal Cashless.pl wraz z Fundacją Fintech Poland **Mapy Polskiego Fintechu**[145] w 2019 r. na polskim rynku działało prawie **200 podmiotów niebankowych**[146], usprawniających operacje finansowe przy wykorzystaniu nowoczesnych technologii. Liczba ta zwiększyła się o około 70 projektów względem 2018 r., co świadczy o bardzo szybkim rozwoju sektora FinTech w Polsce[147].

Dyrektywa PSD2 jako katalizator rozwoju otwartej bankowości

Kluczowym bodźcem dla rozwoju nowych rozwiązań na bazie tradycyjnych usług bankowych jest dyrektywa PSD2. Wprowadziła ona zmianę dotychczasowej działalności dostawców usług płatniczych, w szczególności banków, w kierunku modelu **otwartej bankowości**, zgodnie z którym fintechy działające jako TPP mogą, w imieniu i za zgodą użytkownika, uzyskać dostęp do informacji o jego rachunku płatniczym lub zlecać realizację płatności.

Dyrektywa PSD2 umożliwia tworzenie różnych **modeli kooperacji banków z TPP**. Dopuszcza się współpracę banków z TPP zgodnie z zasadami przewidzianymi w PSD2 bez żadnych uregulowań umownych lub współpracę poprzez zawarcie umowy pomiędzy bankiem a TPP, regulującej w sposób wyczerpujący lub częściowy zasady przyszłej kooperacji.

Współpraca banków z fintechami działającymi w formie start-upów

Otwarcie się banków na podmioty zewnętrzne może być podstawą budowy nowych strategii biznesowych w celu oferowania klientom innowacyjnych rozwiązań. Dzięki współpracy i korzystaniu z otwartej bankowości banki i młode fintechy (start-upy) mogą wykorzystywać swoje mocne strony, polepszając ofertę dla klientów o wiele bardziej niż każdy z tych podmiotów samodzielnie.

Interfejsy API umożliwiają bankom zbieranie przydatnych danych z różnych źródeł, w tym np. informacji o nawykach zakupowych klientów, ich potrzebach finansowych czy poziomach tolerancji ryzyka, a nawet interakcjach społecznych. Informacje uzyskane dzięki tym danym mogą zapewnić bankom bardziej sprofilowany marketing

---

[144] Raport KPMG pt. *Czy klient jest najważniejszy? Na bank!* (październik 2019): https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/10/pl-raport-kpmg-pt-czy-klient-jest-najwazniejszy-na-bank.pdf

[145] https://www.cashless.pl/5906-mapa-polskiego-fintechu-2019-mapa, dostęp z dnia 16.11.2019 r.

[146] Obszary działalności wskazanych podmiotów obejmowały następujące kategorie: płatności, zarządzanie finansami osobistymi, rynki walutowe i handel walutami, pożyczki i kredyty, *middle* lub *back office*, kryptowaluty i *blockchain*, InsurTech, zarządzanie finansami przedsiębiorstwa, cyberbezpieczeństwo.

[147] http://fintechpoland.com/pl/mapa-polskiego-fintechu-2019/, dostęp z dnia 16.11.2019 r.

wielokanałowy, zwiększyć poziom sprzedaży i poprawić jakość świadczonych usług doradczych.

Poniżej przedstawiono główne korzyści wynikające z otwartej bankowości dla banków, fintechów i klientów.

Korzyści dla banków ze strony fintechów
- ✓ Możliwość wprowadzenia innowacyjnych usług lub produktów finansowych.
- ✓ Zwinne podejście we wdrażaniu nowych rozwiązań, ograniczona formalizacja.
- ✓ Dobrze zidentyfikowane potrzeby i oczekiwania klientów.
- ✓ Świeże spojrzenie na wewnętrzne procesy banku pod kątem ich usprawnienia.
- ✓ Efektywne wykorzystywanie danych o klientach, np. w zakresie oceny ryzyka.
- ✓ Unikalna kultura organizacyjna.

Korzyści dla fintechów ze strony banków
- ✓ Szeroka baza klientów.
- ✓ Dostęp do systemu rozliczeń międzybankowych.
- ✓ Duży zasięg działalności (również na arenie międzynarodowej).
- ✓ Wysokie kompetencje w obszarze regulacji, zarządzania ryzykiem i bezpieczeństwa IT.
- ✓ Duże zasoby kapitałowe, możliwość pozyskania finansowania.
- ✓ Większa rozpoznawalność i uznanie na rynku, duże zaufanie wśród klientów.

Korzyści dla klientów wynikające z otwartej bankowości
- ✓ Dostęp do innowacyjnych produktów i usług opartych na bazie najnowszych technologii.
- ✓ Pozytywne doświadczenia klienta (*UX*).
- ✓ Szybkie i wygodne wykonywanie transakcji płatniczych.
- ✓ Lepsze zarządzanie finansami (integracja rachunków płatniczych u różnych dostawców).
- ✓ Łączenie usług bankowych i pozabankowych (np. ubezpieczeniowych).
- ✓ Otrzymywanie konkurencyjnych ofert od różnych instytucji finansowych.

Polskie banki, w szczególności te najbardziej innowacyjne, starają się współpracować z najbardziej rokującymi fintechami, a niektóre z nich mają nawet własne **programy akceleracyjne**. Co więcej, niektóre banki powołały już specjalne komórki organizacyjne ds. współpracy z fintechami, a nawet komórki dedykowane otwartej bankowości, udostępniając specjalne platformy oparte na otwartych interfejsach API, tzw. **sandboxy** (piaskownice), na bazie których mogą być rozwijane nowoczesne rozwiązania[148].

[148] Z dostępnych informacji rynkowych wynika, że polskie banki chętnie angażują się w nowe projekty fintechowe, a młodzi przedsiębiorcy są otwarci na taką współpracę. Wiele start-upów ma interesujące pomysły, ale może nie zaistnieć, dopóki nie stanie za nimi duży „gracz" o ugruntowanej pozycji rynkowej.

W dobie transformacji cyfrowej współpraca banków z fintechami wydaje się nieunikniona i będzie stanowić istotny element strategii biznesowych mających na celu wdrażanie innowacji w usługach finansowych. Co do zasady, wyróżnić można 3 potencjalne formy zaangażowania banków w fintechy:

a) tradycyjne inwestycje w spółkę;
b) przejęcia i fuzje;
c) współpraca partnerska, przy której oba podmioty zostają niezależne, przy czym każdy z partnerów wykorzystuje swoje kluczowe kompetencje.

Banki jako TPP

W związku z dynamicznym rozwojem nowych technologii banki nie tylko będą udostępniać infrastrukturę dla fintechów i z nimi współpracować, ale również same, lub za pośrednictwem podmiotu zależnego, przy spełnieniu określonych warunków, mogą pełnić rolę TPP i oferować klientom nowe usługi dostępu do rachunku[149]. Przykładowo klient danego banku będzie mógł w swojej aplikacji mobilnej (lub serwisie internetowym banku) podłączyć rachunki z innych banków i mieć wgląd do swoich finansów w jednym miejscu (usługa AIS). Ponadto klient będzie mógł zlecać z tych rachunków przelewy zewnętrzne lub pozwolić, aby zewnętrzy dostawca usług (TPP) zlecał w imieniu klienta przelew konkretnemu odbiorcy (usługa PIS).

Otwarta bankowość umożliwia bankom tworzenie i dystrybucję szerokiej gamy nowych, innowacyjnych produktów i usług przy zachowaniu relacji z klientem poprzez tradycyjną bankowość elektroniczną.

W tym miejscu należy wskazać, że zgodnie z art. 2 ustawy Prawo bankowe *bank jest osobą prawną utworzoną zgodnie z przepisami ustaw, działającą na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym*. W świetle tej definicji oraz dalszych przepisów powyższej ustawy nie ulega wątpliwości, że bank jest przedsiębiorcą wykonującym specyficzną działalność gospodarczą (działalność bankową). W myśl art. 3 *Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców*, działalnością gospodarczą jest *zorganizowana działalność zarobkowa, wykonywana we własnym imieniu i w sposób ciągły*. Na tej podstawie za przedmiot (cel) działalności przedsiębiorcy należy uznać te rodzaje działalności, które przedsiębiorca wykonuje w celach zarobkowych, we własnym imieniu w sposób ciągły i które stanowią immanentną, dominującą lub przynajmniej istotną część procesu gospodarczego, skierowaną na stworzenie jego oferty rynkowej. Przedmiotem działania banku są zatem te czynności bankowe i inne dozwolone dla banków rodzaje działalności bankowej, które bank wykonuje w sposób ciągły w ramach realizacji swojego celu gospodarczego (polegającego w skrócie na zarobkowym gromadzeniu depozytów i obciążaniu ich ryzykiem) i które stanowią immanentną, dominującą lub przynajmniej istotną część procesu gospodarczego banku, skierowaną na stworzenie jego oferty rynkowej. Przedmiotu działalności banku nie będą więc w szczególności

[149] W celu świadczenia usług PIS i AIS wymagane są odpowiednie zmiany w statucie banku.

stanowić czynności wykonywane niezarobkowo (np. sponsorowanie imprez sportowych, organizowanie konferencji naukowych), incydentalnie (np. sprzedaż należącej do banku nieruchomości), jak i działalność nienakierowana na stworzenie oferty rynkowej i realizację celu gospodarczego banku, nawet jeżeli działalność ta ma charakter zarobkowy i wykonywana jest w sposób ciągły (np. prowadzenie stołówki pracowniczej). Zakres dopuszczalnej działalności banków został określony w art. 5 ust. 1 i 2 oraz art. 6 ust. 1 ustawy Prawo bankowe. W art. 5 ust. 1 i 2 zostały wymienione czynności bankowe *sensu stricto* (ust. 1) oraz czynności uznawane za bankowe, gdy są wykonywane przez banki (ust. 2). Banki mogą też wykonywać czynności inne niż bankowe, wskazane w art. 6 ust. 1 ustawy Prawo bankowe. **Katalog czynności dozwolonych do wykonywania przez banki jest zamknięty**, co oznacza, że banki mogą w ramach przedmiotu działalności wykonywać jedynie czynności wymienione w przywołanych wyżej przepisach, względnie inne czynności na podstawie art. 6 ust. 1 pkt 8 – wskazane w przepisach odrębnych.

Powyższe może mieć istotne znaczenie w przypadku świadczenia przez banki występujące w roli TPP tzw. **usług premium** rozwijanych w szczególności na bazie usługi AIS umożliwiającej dostęp do informacji o rachunkach płatniczych klientów.

Jak bowiem wynika z powyższych wyjaśnień dotyczących przedmiotowego zakresu działalności banków, świadczenie przez banki usług premium na bazie usługi AIS jest dopuszczalne pod warunkiem, że usługi te będą mieściły się w katalogu czynności możliwych do wykonywania przez banki w świetle przepisów prawa.

Wspólne standardy komunikacji

W myśl zapisów dyrektywy PSD2 istotnym elementem rozwoju otwartej bankowości jest zapewnienie interoperacyjności i współdziałania różnych rozwiązań komunikacyjnych. Otwarte interfejsy API budowane po stronie banków powinny umożliwiać korzystanie ze wszystkich powszechnie dostępnych rodzajów urządzeń, takich jak komputery, tablety czy smartfony.

Standard PolishAPI[150], który został opracowany pod auspicjami Związku Banków Polskich, we współpracy z uczestnikami rynku, spełnia wymogi wynikające z dyrektywy PSD2 i pozwala na projektowanie szeregu nowych usług dla klientów na bazie interfejsów API.

Zdecydowana większość polskich banków udostępniła swoje portale deweloperskie lub strony internetowe zapewniające dostęp do wdrożonych interfejsów komunikacji z TPP w oparciu o standard PolishAPI. Jest to kluczowy moment, kiedy TPP po raz pierwszy mogą sięgnąć po „dane bankowe" i jednocześnie być odpowiedzialnym za ich ochronę na równi z instytucjami bankowi.

[150] Więcej informacji nt. standardu PolishAPI przedstawiono w rozdziale 6.

Kierunki rozwoju otwartej bankowości

Na wstępie należy wskazać, że rozwój otwartej bankowości to proces ciągły, który wymaga odpowiednich zmian zarówno po stronie uczestników rynku, jak również samych klientów. W dniu 14 września 2019 r., w którym zaczęły w pełni obowiązywać przepisy RTS, nie pojawiły się od razu na polskim rynku nowe rozwiązania z obszaru otwartej bankowości, co nie oznacza, że z biegiem czasu klienci nie będą mieli dostępu do coraz szerszego katalogu nowych usług[151].

Wiele wskazuje na to, że otwarta bankowość w pierwszej kolejności będzie rozwijana w Polsce głównie przez banki oraz instytucje płatnicze i umożliwi oferowanie **usług AIS opartych na analizie danych**, a także produktów związanych z zarządzaniem domowym budżetem i finansami osobistymi klientów. Można również oczekiwać rozwoju nowych **rozwiązań płatniczych w ramach usługi PIS**.

Analizując koncepcję otwartej bankowości, należy zadać pytanie, czy banki widzą realne zagrożenie ze strony fintechów, w szczególności ze strony innowacyjnych start-upów. Na podstawie przygotowanego raportu Związku Banków Polskich i KPMG[152] okazuje się, że ponad 40% ankietowanych banków postrzega **inne banki** jako swoją największą konkurencję w początkowej fazie wdrożenia wymogów dyrektywy PSD2. Z kolei aż 53% ankietowanych banków wskazuje **firmy z sektora BigTech**, występujące pod akronimem **GAFA** (Google, Apple, Facebook, Amazon)[153], jako największe zagrożenie w ciągu najbliższych kilku lat. Technologiczne giganty coraz bardziej ukierunkowują swoje działania w celu świadczenia usług finansowych, głównie w obszarze płatności. Podmioty te posiadają ogromną bazę klientów, duże doświadczenie w cyfrowych modelach działalności i potężne zaplecze technologiczne oparte m.in. na chmurze obliczeniowej (ang. *cloud computing*), co w wielu przypadkach umożliwia im kreowanie dużo wyższych wartości dla klientów niż banki, ubezpieczyciele, firmy inwestycyjne, instytucje płatnicze, a nawet małe, zwinne fintechy.

Z drugiej strony wnioski z raportu ZBP i KPMG[154] wskazują na to, że **zaufanie do firmy nie jest tożsame z chęcią powierzania jej danych do logowania do banku czy też udostępniania danych transakcyjnych**. Wg wyników badania konsumenci ufają bankom (41%), Google (38%) i Facebookowi (22%) w dość znaczącym stopniu. Natomiast dostęp do danych transakcyjnych udostępni tym firmom już znacząco niższy procent respondentów: banki (32%), Google (3%), Facebook (2%).

Wraz z upływem czasu skłonność do udostępniania danych transakcyjnych podmiotom innym niż banki będzie wzrastać z uwagi na **zmianę pokoleniową**. Można

---

[151] https://fintek.pl/bilans-psd2-po-trzech-dniach/, dostęp z dnia 16.11.2019 r.

[152] Raport Związku Banków Polskich i KPMG pt. *PSD2 i Open Banking. Rewolucja czy ewolucja?*, Marzec 2019.

[153] W pytaniu ankietowym nie uwzględniono chińskich gigantów technologicznych zaliczanych do sektora BigTech, którzy występują pod akronimem BAT (Baidu, Alibaba, Tencent). W niektórych opracowaniach stosuje się również rozszerzony akronim GAFAA, który uwzględnia firmę Alibaba.

[154] Ibidem.

to zaobserwować na przykładzie postrzegania przez osoby w wieku 18–24 lat wizerunku firm technologicznych w porównaniu do starszego pokolenia. Już sam przykład udostępnienia danych transakcyjnych ilustruje, jak różnie podchodzą do tej kwestii te 2 grupy. Przykładowo, na podstawie przeprowadzonego badania[155] firmie Google udostępni swoje dane ponad 9% respondentów w wieku 18–24 lat, 4% w grupie wiekowej 25-39, 3% badanych w przedziale 40–59 lat i 1% respondentów, którzy mają powyżej 60 lat. To oznacza, że w najbliższych latach rzeczywiście może powstać rynek dla firm z sektora BigTech na świadczenie usług w oparciu o otwartą bankowość.

W dłuższej perspektywie otwarta bankowość znacząco zmieni sektor bankowy i cały rynek usług finansowych w Polsce. Aby sprostać nadchodzącym wyzwaniom, banki powinny skupiać się na rozwijaniu dodatkowych źródeł przychodów, tworząc nowe modele współpracy z fintechami i innymi partnerami, wchodząc jednocześnie w rolę TPP. Nie należy również wykluczać potencjalnej **współpracy banków z firmami z sektora BigTech**, które posiadają bardzo dużą bazę klientów, ale może im brakować wiarygodnego źródła potwierdzającego tożsamość tych klientów, a w tej domenie od wielu lat specjalizują się banki.

Nadchodzi *Open X*

Mimo iż otwarta bankowość nie osiągnęła jeszcze dojrzałości, sektor usług finansowych równolegle będzie wkraczał w nową fazę innowacji, określaną jako ***Open X***. Założeniem funkcjonowania *Open X* jest **głębsza współpraca pomiędzy uczestnikami rynku oparta na specjalizacji oraz poprawa standaryzacji interfejsów API** w celu ograniczenia skali oszustw, zapewnienia większej interoperacyjności, lepszej jakości obsługi klienta i szybszego wprowadzania innowacji produktowych. Nadejście *Open X* napędzane jest 4 głównymi zmianami[156]:

a) odejściem od koncentracji na produktach i zaakcentowaniem doświadczenia klienta (UX),
b) ewolucją danych jako krytycznego zasobu,
c) przejściem od priorytetu własności do wspierania wspólnego dostępu,
d) położeniem nacisku na partnerstwo w celu wprowadzania innowacji zamiast na kupowanie lub budowanie nowych rozwiązań.

W związku z nadchodzącą nową fazą innowacji uczestnicy *Open X* będą musieli wybrać strategiczne role w ramach określonych specjalizacji. W szczególności pojawią się **dostawcy** (ang. *suppliers*), którzy będą opracowywać nowoczesne produkty i usługi, **agregatorzy** (ang. *aggregators*), którzy je zgromadzą i rozdystrybuują, utrzymując relacje z klientami, a także **orkiestratorzy** (ang. *orchestrators*), którzy będą pełnić rolę łączników rynkowych i koordynatorów, ułatwiając interakcje pomiędzy partnerami. W powyższej koncepcji nie będzie już miejsca dla podmiotów, które nie otworzą się na współpracę i nie obiorą jednej z ról, w której będą miały najwyższe kompetencje[157].

[155] Ibidem.
[156] *World FinTech Report* (WFTR) 2019, https://www.capgemini.com/pl-pl/news/world-fintech-report-2019/
[157] Ibidem.

***Open X* przekształci sektor usług finansowych we wspólny ekosystem lub rynek z nowym pakietem produktów i usług w ramach wyodrębnionych specjalizacji**, wobec czego zarówno banki, jak i fintechy będą musiały redefiniować swoją strategię rozwoju innowacji i obsługi klientów, pozyskując przy tym wysoko wykwalifikowaną kadrę pracowniczą w zakresie nowych technologii.

ZAKOŃCZENIE

Dyrektywa PSD2, która została wdrożona do systemu prawnego w Polsce i innych krajach Unii Europejskiej, umożliwiła nieregulowanym wcześniej niebankowym podmiotom trzecim (TPP) dostęp do rachunków płatniczych użytkowników. To sprawiło, że na rynku usług finansowych rozpoczęła się era otwartej bankowości, w ramach której wokół tradycyjnych instytucji finansowych zaczął powstawać cały ekosystem nowych firm, zwanych potocznie fintechami, oferujących produkty i usługi w oparciu o dostęp do danych przetwarzanych do tej pory tylko przez same banki.

Kluczowym aktem prawnym uzupełniającym dyrektywę PSD2 są regulacyjne standardy techniczne (RTS), określające wymogi w zakresie silnego uwierzytelniania klienta oraz wspólnych i bezpiecznych otwartych standardów komunikacji. RTS stawiają przed uczestnikami rynku wiele wyzwań natury regulacyjnej i biznesowej, z którymi muszą zmierzyć się przede wszystkim dostawcy usług płatniczych prowadzący rachunki użytkowników (ASPSP), w szczególności banki.

Wymogi RTS powinny być w pełni stosowane od dnia 14 września 2019 r[158]. Dużym wyzwaniem dla ASPSP może być **właściwe wdrożenie procedury silnego uwierzytelniania klienta (SCA)** w zakresie oferowanych produktów i usług, tj. wprowadzenie zabezpieczenia pozwalającego na zminimalizowanie ryzyka nieuprawnionego dostępu do rachunku płatniczego i wykonania nieautoryzowanej transakcji. Taka implementacja oznacza koszty oraz zaangażowanie wielu jednostek biznesowych ASPSP, ale daje również możliwość przeglądu dotychczasowej oferty produktowej pod kątem zastosowania innowacyjnych rozwiązań. ASPSP powinny komunikować swoim klientom, że celem wprowadzenia SCA jest przede wszystkim zwiększenie poziomu bezpieczeństwa usług bankowości elektronicznej. W niektórych przypadkach procedura SCA może wydłużyć czas autoryzacji transakcji lub dostępu do rachunku, ale należy pamiętać, że procesy te będą stopniowo przyśpieszać z uwagi na coraz częstsze wykorzystywanie metod weryfikacji tożsamości klienta opartych na danych biometrycznych.

Kolejnym kluczowym wyzwaniem dla ASPSP wynikającym z RTS jest **zapewnienie sprawnie działającego, wydajnego i skalowalnego interfejsu API na potrzeby komunikacji z TPP** (w tym środowiska testowego oraz produkcyjnego) wraz z niezbędną dokumentacją opisującą zasady integracji TPP z infrastrukturą informatyczną ASPSP. Istotnym zagadnieniem dla wielu ASPSP jest uzyskanie zgody KNF na zwolnienie z tzw. **opcji *fallback***, w ramach której TPP na wypadek awarii lub niedostępności API może korzystać z tradycyjnego interfejsu użytkownika przeznaczonego do komunikacji z ASPSP. Należy bowiem pamiętać, że jednym z warunków uzyskania takiej zgody jest

[158] Zgodnie z *Komunikatem KNF z dnia 19 sierpnia 2019 r. w sprawie silnego uwierzytelniania klienta w przypadku niektórych form płatności przy użyciu instrumentów płatniczych* oraz opinią EBA z dnia 16 października 2019 r. termin na spełnienie niektórych wymogów w zakresie silnego uwierzytelniania klienta, pod pewnymi warunkami, może zostać wydłużony.

powszechne stosowanie API przez TPP w co najmniej 3-miesięcznym okresie. W początkowej fazie rozwoju otwartej bankowości ASPSP mogą spotkać się z problemem braku dostatecznej aktywności TPP na rynku polskim. W takiej sytuacji organ nadzoru będzie brał pod uwagę wszystkie działania podejmowane przez ASPSP, które miały na celu zachęcić TPP do korzystania z udostępnionego interfejsu.

Oprócz wyzwań stojących przed ASPSP należy również wskazać na wyzwania, z którymi będą mierzyć się TPP planujące dopiero wejść na regulowany rynek finansowy. W pierwszej kolejności takie podmioty muszą uzyskać **odpowiednie zezwolenie/rejestrację organu nadzoru na świadczenie wybranych usług dostępu do rachunku** (PIS, AIS, CAF). Dodatkowo TPP muszą dostosować swoje środowiska informatyczne do interfejsów ASPSP, ale również pozyskać kwalifikowane certyfikaty eIDAS, aby móc się identyfikować względem ASPSP. Ponadto, biorąc pod uwagę wieloletnie przyzwyczajenia i wysokie zaufanie klientów do banków, zapewne **TPP będą musiały edukować klientów**, że korzystanie z TPP jest również bezpieczne i może przynieść szereg różnych korzyści. Doświadczenia Wielkiej Brytanii po wdrożeniu PSD2 pokazały, że bardzo dużym wyzwaniem dla TPP okazała się niska świadomość klientów banków, którzy na początku nie zdawali sobie sprawy, czym jest i co dla nich oznacza otwarta bankowość i czy mogą udostępniać swoje dane innym firmom niż ich główny bank.

Niezależnie od powyższego należy również wskazać, że **rolę TPP będą pełniły także same banki**, które od wielu lat budują zaufanie wśród klientów, i to w nich pokłada się największe nadzieje na początkowy rozwój otwartej bankowości na polskim rynku. Dzięki dostępowi do danych klientów, udostępnianych przez inne banki za pośrednictwem API, banki działające jako TPP będą mogły zwiększyć atrakcyjność swoich produktów finansowych i oferować nowe rozwiązania w oparciu o dane pozyskiwane z zewnętrznych źródeł. Należy przy tym zauważyć, że **wiele banków postrzega inne banki (a nie prężnie rozwijające się młode fintechy) jako swoją największą konkurencję** w początkowej fazie wdrożenia wymogów dyrektywy PSD2. Należy również pamiętać, że **znaczącą rolę w otwartej bankowości mogą odgrywać największe firmy technologiczne z sektora BigTech**, które od wielu lat specjalizują się w personalizacji produktów i budowaniu pozytywnych doświadczeń klienta (UX).

Dużym wyzwaniem dla wszystkich podmiotów działających w ramach otwartej bankowości są **potencjalne zagrożenia płynące z cyberprzestrzeni**. Podstawowym elementem zapewnienia bezpieczeństwa użytkowników usług płatniczych jest **właściwa ochrona ich indywidulanych danych uwierzytelniających i autoryzacyjnych**. Jeśli obniży się poziom bezpieczeństwa i wzrośnie odsetek oszustw w Internecie, może to wywołać ogólny spadek zaufania do usług bankowości elektronicznej. Bezpieczeństwo danych użytkowników powinno wynikać nie tylko z samych regulacji, ale również z działań podejmowanych przez odpowiednie komórki zarządzania ryzykiem, kontroli wewnętrznej, w tym audytu i funkcji zapewnienia zgodności (ang. *compliance*). **ASPSP będą musiały zmierzyć się również z trudnym zagadnieniem ewentualnej odmowy TPP dostępu do API**, w szczególności wobec rosnącej liczby cyberataków. W takim przypadku istotne będą odpowiednie procedury bezpieczeństwa,

w tym właściwa identyfikacja TPP, oraz bieżące monitorowanie ryzyk i pojawiających się zagrożeń.

Należy jednocześnie pamiętać, że nawet najlepszy standard komunikacji z TPP nie ograniczy oszustw opartych na *phishingu*, jeżeli użytkownik nie będzie sam przestrzegał podstawowych zasad bezpieczeństwa. Dlatego **bardzo ważne jest edukowanie użytkowników**, aby nie stracili oni czujności podczas udostępniania swoich danych. Wszystkie usługi świadczone przez TPP mogą być realizowane tylko za wyraźną zgodą użytkownika. Oznacza to, że **użytkownik powinien być świadomy, komu i w jakim zakresie udziela zgody na świadczenie danej usługi**. Forma przedstawiania użytkownikowi informacji o usłudze powinna być jak najbardziej czytelna, aby mógł on dokładnie zapoznać się z warunkami świadczenia usługi, zanim zacznie z niej korzystać.

W kontekście potrzeby zapewnienia bezpieczeństwa **otwarta bankowość kreuje również nowe wyzwania dla nadzoru finansowego**. Rosnąca liczba ataków na użytkowników bankowości internetowej i mobilnej powoduje, że KNF bardzo uważnie przygląda się nowym rozwiązaniom technologicznym, podejmując jednocześnie działania na rzecz rozwoju innowacji na rynku finansowym[159]. **Ryzyka związane z nowymi technologiami wysuwają się w działalności instytucji finansowych na jedną z kluczowym pozycji**, dlatego ASPSP, wdrażając nowe rozwiązania, powinny efektywnie zarządzać ryzykami zarówno po swojej stronie, jak i po stronie klienta, w szczególności w obszarze jego infrastruktury (np. w zakresie ochrony przed złośliwym oprogramowaniem aplikacji bankowych instalowanych na urządzeniach przenośnych klientów). KNF od dłuższego czasu zwraca uwagę banków na konieczność zapewnienia bezpieczeństwa w bankowości elektronicznej, w tym w bankowości mobilnej. Jest to kanał, który w ostatnim czasie rozwija się bardzo dynamicznie, a w ślad za tym pojawiają się nowe zagrożenia, które KNF na bieżąco monitoruje i analizuje, aby móc podejmować odpowiednie środki nadzorcze.

Istotnym wyzwaniem dla podmiotów działających w modelu otwartej bankowości jest także **wspieranie inkluzji finansowej**[160]. Rozwój nowych, często skomplikowanych usług i produktów może w niektórych przypadkach prowadzić do pogłębiania wykluczenia cyfrowego i finansowego (ang. *financial exclusion*) tej części społeczeństwa, która z różnych przyczyn nie może korzystać z dostępu do najnowszych technologii (np. nie posiada smartfona z dostępem do Internetu[161]).

---

[159] Przykładem jest Program Innovation Hub, w ramach którego UKNF prowadzi dialog z podmiotami sektora FinTech, udzielając im stosownych wyjaśnień na zadane zapytania, wspierając tym samym rozwój nowoczesnych technologii na rynku finansowym przy zachowaniu bezpieczeństwa i odpowiedniej ochrony klientów. Zasady działania Programu dostępne są na stronie KNF: https://www.knf.gov.pl/dla_rynku/fin_tech/Innovation_Hub

[160] Inkluzja finansowa (ang. *financial inclusion*) oznacza umożliwienie szerokiego dostępu różnym grupom społecznym (a zwłaszcza tym o niższych dochodach) do bezpiecznych, wygodnych i niedrogich produktów i usług finansowych.

[161] Na podstawie opracowania autorstwa Faith Reynolds pt. *Open Banking, A Consumer Perspective* (str. 22), 2017, zrealizowanego na zlecenie Barclays Bank: https://www.openbanking.org.uk/wp-content/uploads/Open-Banking-A-Consumer-Perspective.pdf

Innym wyzwaniem związanym z rozwojem otwartej bankowości jest **wdrożenie na poziomie paneuropejskim wystandaryzowanej procedury rozwiązywania ewentualnych sporów pomiędzy ASPSP a TPP** w określonych ramach czasowych, co przyczyniłoby się do wzrostu efektywności funkcjonowania nowej koncepcji. Źródła tego rodzaju sporów wszczynanych przez TPP mogą leżeć np. w czasowych brakach dostępu TPP do rachunku klienta, wywołanych problemami technicznymi po stronie banku. Z kolei źródłem sporów inicjowanych przez banki może być, dla przykładu, wyciek danych uwierzytelniających klientów spowodowany przez TPP czy też w wyniku reklamacji klientów próby dochodzenia przez banki od TPP odpowiedzialności za transakcje nieautoryzowane wykonywane za pośrednictwem TPP[162].

Podsumowując, można stwierdzić, że **w dłuższej perspektywie otwarta bankowość znacząco zmieni cały rynek usług finansowych w Polsce, przynosząc korzyści zarówno klientom, bankom, jak i fintechom**. Klienci będą mogli otrzymywać dostosowane do ich indywidualnych potrzeb oferty usług bankowych i pozabankowych. Banki, poprzez współpracę z fintechami, będą mogły adaptować nowe technologie, ale również same pełnić rolę TPP, oferując nowe usługi dostępu do rachunku. Dla fintechów korzyścią wynikającą ze współpracy z bankami będzie dostęp do szerokiej bazy klientów i infrastruktury płatniczej, zwiększenie wiarygodności i możliwość pozyskania finansowania na ich dalszy rozwój.

Mimo iż otwarta bankowość nie osiągnęła jeszcze docelowego poziomu rozwoju, sektor usług finansowych będzie jednocześnie wkraczał w nową fazę innowacji, określaną jako ***Open X***, której założeniem jest **głębsza współpraca pomiędzy uczestnikami rynku, oparta na specjalizacji**, jak również **poprawa standaryzacji interfejsów API** w celu redukcji oszustw, zapewnienia większej interoperacyjności, wyższej jakości obsługi klienta oraz szybszego wprowadzania innowacyjnych produktów i usług.

[162] Więcej informacji nt. wyzwań stojących przed bankami i organami nadzoru w związku z pojawieniem się otwartej bankowości można znaleźć w raporcie Banku Rozrachunków Międzynarodowych (ang. *Bank for International Settlements* – BIS) pt. *Report on open banking and application programming interfaces* (listopad, 2019): https://www.bis.org/bcbs/publ/d486.pdf

REGULACJE PRAWNE I WYTYCZNE NADZORCZE ISTOTNE DLA OTWARTEJ BANKOWOŚCI

UNIJNE AKTY PRAWNE

1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (PSD2).

2) Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji. Obowiązuje od dnia 14 września 2019 r. (RTS).

3) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO).

4) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

KRAJOWE AKTY PRAWNE

5) Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. z 2019 r. poz. 659 t.j. z późn. zm.).

6) Rozporządzenie Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 61b ust. 1 ustawy o usługach płatniczych (Dz.U. z 2019 r. poz. 1459).

7) Rozporządzenie Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 117a ust. 3 ustawy o usługach płatniczych (Dz.U. z 2019 r. poz. 1458).

8) Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2018 r. poz. 2187 t.j. z późn. zm.).

9) Ustawa z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (Dz.U. z 2018 r. poz. 613, z 2019 r. poz. 730. t.j.).

10) Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2012 r. poz. 855 z późn. zm.).

11) Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. z 2019 r. poz. 1292 t.j. z późn. zm.).

12) Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2019 r. poz. 1115 t.j. z późn. zm.).

13) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 z późn. zm.).

14) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2019 r. poz. 162 t.j. z późn. zm.).

OPINIE I WYTYCZNE EBA

15) Wytyczne EBA z dnia 8 listopada 2017 r. dotyczące informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 PSD2 (EBA/GL/2017/09).
https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PL.pdf/06b0a678-eccb-4d58-8268-e0e22b0c3c23

16) Wytyczne EBA z dnia 19 grudnia 2017 r. dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2) (EBA/GL/2017/10).
https://eba.europa.eu/sites/default/documents/files/documents/10180/2066978/5a5de98d-8cbf-4fb4-99ce-67556a129b8b/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10)_PL.pdf

17) Wytyczne EBA z dnia 12 stycznia 2018 r. w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy PSD2 (EBA/GL/2017/17).

https://eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_PL.pdf/cd60445e-e39b-413a-b297-6a8bedcf7dc2

18) Opinia EBA z dnia 13 lipca 2018 r. dotycząca implementacji regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (EBA-Op-2018-04) (ang.).
https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

19) Wytyczne EBA z dnia 17 września 2018 r. w sprawie wymogów zgłaszania nadużyć finansowych na podstawie art. 96 ust. 6 drugiej dyrektywy PSD2 (EBA/GL/2018/05).
https://eba.europa.eu/documents/10180/2352765/Guidelines+on+fraud+reporting+%28EBA+GL-2018-05%29_PL.pdf/2e81c374-e36b-409f-a56c-c506fd46c2b5

20) Wytyczne EBA z dnia 4 grudnia 2018 r. w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji) (EBA/GL/2018/07).
https://eba.europa.eu/documents/10180/2570450/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back_PL.pdf/0580ad7a-3c40-48ef-9d86-71c15245eabc

21) Opinia EBA z dnia 10 grudnia 2018 r. dotycząca zastosowania certyfikatów eIDAS w związku z RTS (EBA-Op-2018-7) (ang.).
https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf

22) Opinia EBA z dnia 21 czerwca 2019 r. dotycząca elementów silnego uwierzytelniania klienta (EBA-Op-2019-06) (ang.).
https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

23) Opinia EBA z dnia 16 października 2019 r. dotycząca terminu migracji do rozwiązań zgodnych z SCA w zakresie internetowych transakcji płatniczych w obszarze e-commerce (EBA-Op-2019-11) (ang.).
https://eba.europa.eu/documents/10180/2622242/Opinion+on+the+deadline+for+the+migration+to+SCA.pdf

24) Wytyczne EBA z dnia 28 listopada 2019 r. w sprawie zarządzania ryzykiem teleinformatycznym (ICT) oraz bezpieczeństwa (EBA/GL/2019/04) (ang.).

https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

25) Opinie EBA w ramach sekcji pytań i odpowiedzi (Single Rulebook Q&A) w zakresie PSD2/RTS (ang.).
https://eba.europa.eu/single-rule-book-qa

OPINIE I WYTYCZNE KNF/UKNF

26) Komunikat UKNF z dnia 12 stycznia 2018 r. dotyczący wybranych oczekiwań nadzorczych w odniesieniu do okresu przejściowego związanego z implementacją dyrektywy PSD2.
https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_w_sprawie_PSD2_60678.pdf

27) Komunikat UKNF z dnia 31 października 2018 r. w sprawie obowiązku raportowania przez dostawców usług płatniczych informacji o incydentach na podstawie PSD2.
https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ws_raportowania_incydentow_na_podstawie_PSD2_63638.pdf

28) Komunikat UKNF z dnia 1 lipca 2019 r. w sprawie zwolnienia z tzw. opcji fallback.
https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_Urzedu_KNF_w_sprawie_zwolnienia_z_tzw_opcji_fallback.pdf

29) Komunikat KNF z dnia 19 sierpnia 2019 r. w sprawie silnego uwierzytelniania klienta w przypadku niektórych form płatności przy użyciu instrumentów płatniczych.
https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_KNF_w_sprawie_silnego_uwierzytelniania_klienta_66811.pdf

30) Ostrzeżenie UKNF z dnia 6 września 2019 r. dot. wyłudzania poufnych informacji w zw. z PSD2.
https://www.knf.gov.pl/o_nas/komunikaty?articleId=66987&p_id=18

KNF | CEDUR
Centrum Edukacji dla
Uczestników Rynku

ISBN 978-83-66322-03-5

Urząd Komisji Nadzoru Finansowego
ul. Piękna 20
00-549 Warszawa
tel. (+48) 22 262 50 00
fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl