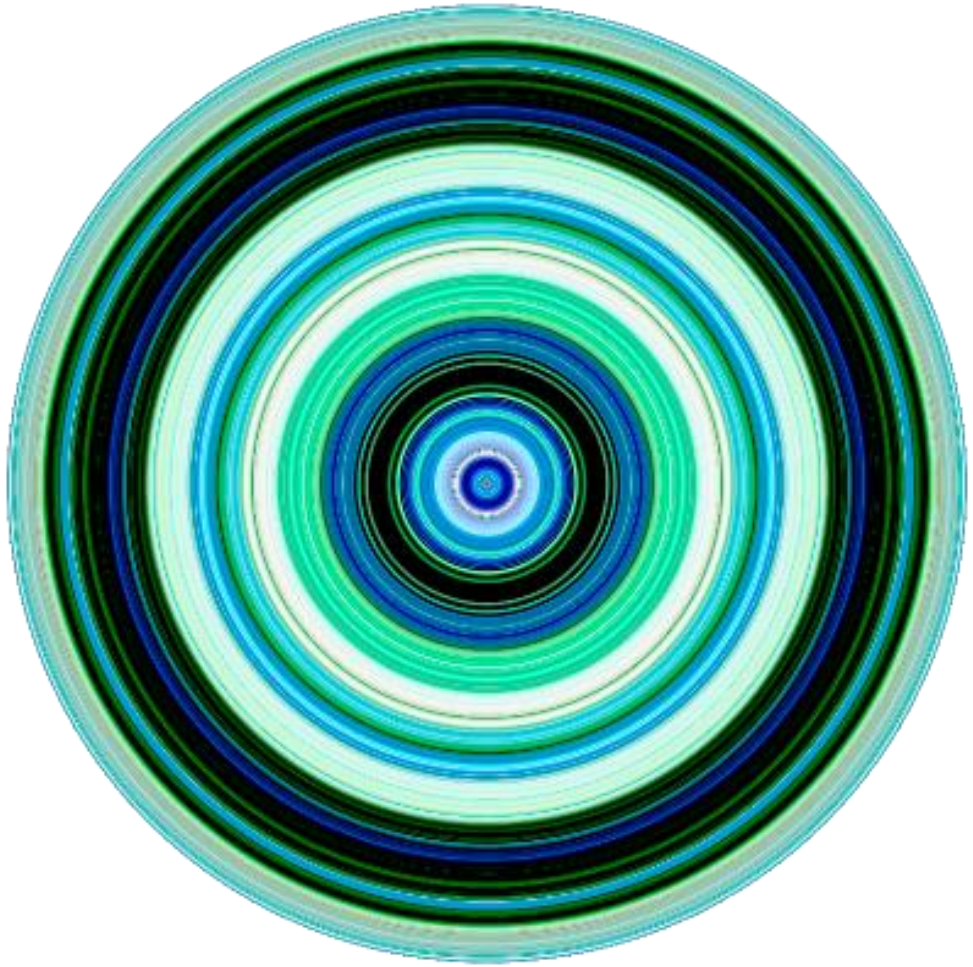
Deloitte.

KONGRES BANKOWOŚCI DETALICZNEJ



Dyrektywa PSD2

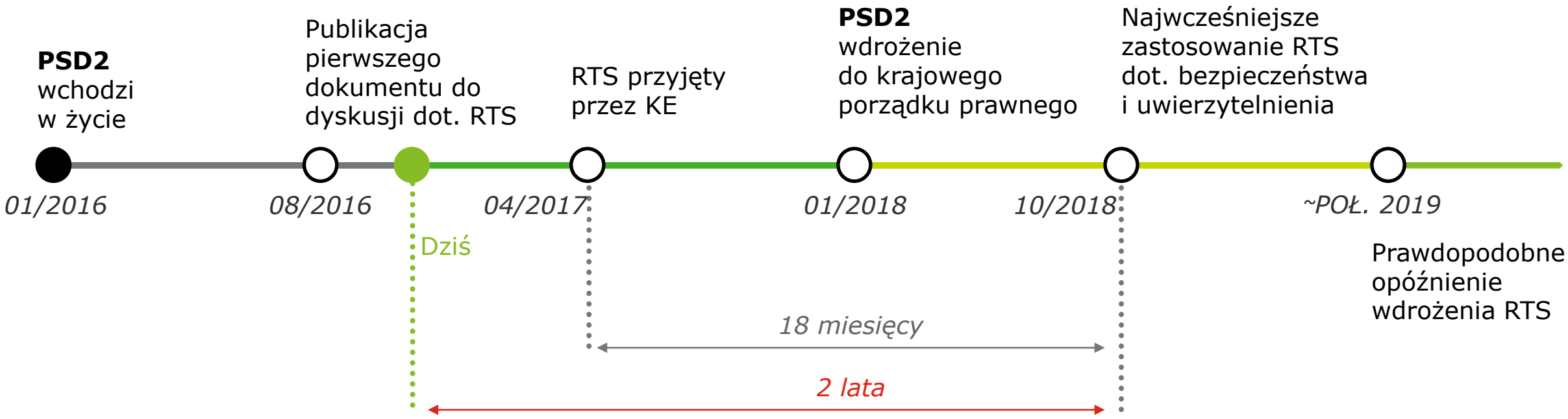
Wprowadzenie do dyskusji

24 listopada 2016r.

PSD2
Zakres nowych wymogów

Zakres nowych wymogów

Harmonogram wdrożenia i główne daty



PSD2: Dyskusje do 01/2017, następnie do połowy 2017 finalizacja.
Wejście w życie **01/2018**

RTS: Przekazanie przez EBA do Komisji Europejskiej 13/01/2017 KE przyjmuje w 04/2017.
Wejście w życie **04/2017 + 18 miesięcy**

Zakres nowych wymogów

Bazując na podstawach określonych w PSD, PSD2 ma na celu dalszy wzrost konkurencji oraz innowacji na rynku płatniczym

PSD1
Wprowadzenie postaw

- Pierwotna dyrektywa w sprawie usług płatniczych (PSD) została uchwalona w 2007 roku i stworzyła bazę prawną dla Jednolitego Obszaru Płatności (SEPA)
- Celem PSD było zwiększenie:
  - konkurencji w ramach EU
  - ochrony konsumentów
  - praw i obowiązków dostawców usług płatniczych

PSD2
Uzupełnienie brakujących komponentów

- PSD2 rozszerza zakres PSD w celu dalszego wzrostu konkurencji i innowacji na rynku płatniczym

Rozszerzenie zakresu obowiązywania

Objęcie dostawców usług płatniczych

Bezpieczeństwo i uwierzytelnianie

Rozszerzenie zakresu

PSD2 obejmuje także transakcje ‘one leg out’, tzn. we wszystkich walutach oraz także przy transakcjach wykraczających poza europejski obszar gospodarczy (w części procesowanej w EU)

Bezpieczeństwo

PSD2 wprowadza nowe wymogi dotyczące bezpieczeństwa w zakresie dostępu do rachunku i autoryzacji płatności oraz zawiera szereg wytycznych w tym zakresie, które muszą wypełnić PISP I AISP

Dostawca świadczący usługę inicjowania płatności (PISP)

PSD2 pozwala inicjować transakcje płatnicze z rachunków bankowych nie tylko poprzez bezpośrednie zalogowanie się do systemu bankowego przez klienta, ale również za pośrednictwem PISP, który przekazuje instrukcje płatnicze do banku prowadzącego rachunek klienta

Dostawca świadczący usługi dostępu do informacji o rachunku (AISP)

PSD2 zawiera zasady otwierające dostęp do informacji dotyczących rachunków płatniczych dla stron trzecich za pośrednictwem AISP, zwiększając zasięg i znaczenie agregatorów informacji płatniczych

Zakres nowych wymogów
PISP, AISP – zakres dostępu

- PSD2 umożliwia dostęp do rachunków płatniczych, które są dostępne on-line
- Rachunki płatnicze są najczęściej prowadzone przez bank lub innych wydawców kart kredytowych (=ASPSP*)
- Inne typy rachunków (np. kredytowe, inwestycyjne) nie są objęte zakresem PSD2 (czyli PSD2 ≠ wszystkie produkty bankowe dostępne on-line)
- PISP powinien otrzymać dostęp do informacji niezbędnych do zainicjowania transakcji, weryfikacji rachunku oraz weryfikacji, czy saldo na rachunku jest wystarczające do dokonania transakcji

- Zgodnie z PSD2 saldo oraz transakcje na rachunkach płatniczych, dla których klient da zgodę, muszą być udostępnione AISP przez ASPSP (bank)**
- PSD2 RTS*** definiuje, że AISP może zapytywać o informacje dot. rachunku płatniczego zawsze, kiedy klient aktywnie potrzebuje dostępu do informacji, lub maksymalnie 2 razy w ciągu dnia w innych przypadkach
- Wg PSD2 RTS AISP nie może wykorzystywać informacji dla celów innych niż wykonanie świadczonej usługi

*ASPSP = Account Servicing Payment Service Provider / dostawca usług płatniczych prowadzący rachunek

**Uwaga: Bank może odmówić dostępy dostawcom usług płatniczych, w przypadku podejrzanych, potencjalnie nieautoryzowanych transakcji

***RTS = Regulatory Technical Standards (dla PSD2) / regulacyjne standardy techniczne

Zakres nowych wymogów
Główne obszary wpływu

Dostosowanie systemów centralnych

Implementacja interfejsu API wraz z odpowiednimi funkcjonalnościami może się okazać złożona i kosztowna, w zależności od istniejących podstawowych systemów bankowych i procesów.

Standard komunikacji, uwierzytelnianie bezpieczeństwo

Jednym z głównych celów PSD2 jest zbudowanie otwartego systemu wymiany danych i informacji. Będzie wymagało to wypracowania odpowiednich standardów wymiany danych.

PSD2 wprowadza pojęcie silnego uwierzytelniania klienta (strong customer authentication).

Odpowiedzialność

ASPSP (banki) będą odpowiedzialni przed klientem także w przypadku transakcji płatniczych zlecanych za pośrednictwem PISP, kiedy błąd może nastąpić w wyniku działania PISP.

TPP będą musiały zarekomendować bankom ewentualne odszkodowania dla klientów (D+1).

Strategia biznesowa

Nadanie dostępu do rachunków podmiotom trzecim powinno być połączone z opracowaniem strategii cyfrowej w bankach.

Jednocześnie PSD2 stwarza dodatkowe możliwości dla dostawców specjalistycznych usług płatniczych, technologicznym gigantom jak i internetowym pożyczkodawcom.

PSD2

Standardy komunikacji i bezpieczeństwo

Standardy komunikacji i bezpieczństwo

Regulacyjne Standardy Techniczne (RTS) – dostęp do rachunku (XS2A) i standardy komunikacji

- RTS wymaga, aby ASPSP (banki) udzieliły dostępu PISP i AISP poprzez dedykowany interfejs programistyczny (API) lub przez istniejący intefejs bankowości internetowej
- RTS nie wprowadza ujednoliconego standardu rynkowego API, a jedynie zaleca stosowanie standardu ISO 20022
- Interfejs banku musi oferować takie same funkcjonalności jak portal internetowy banku zarówno w zakresie realizacji płatności jak i dostępu do rachunku
- Dostęp do rachunku (XS2A) musi się odbywać za pomocą silnego uwierzytelniania (strong customer authentication)
- TPP może dostać dostęp do rachunku wyłącznie po uzyskaniu zgody klienta
- PISP są zobowiązane do identyfikowania siebie przed ASPSP przy każdorazowym zleceniu płatności oraz do rejestracji przy właściwych organach kraju członkowskiego

Standardy komunikacji i bezpieczństwo

Dostęp do rachunku (XS2A) oraz silne uwierzytelnianie (SCA)

- ASPSP (bank) definiuje procedury bezpieczeństwa dla procesu inicjacji transakcji płatniczej
- EBA ograniczyła wyjątki dot. silnego uwierzytelniania do bezdotykowych płatności kartowych poniżej €50, transakcji poniżej €10 oraz płatności do odbiorców wskazanych jako zaufani
- Silne uwierzytelnienie powinno zawierać mechanizmy zapobiegania, wykrywania i blokowania nieuprawnionych płatności (fraudy) przed ostateczną autoryzacją płatności

SCA wymaga zastosowania dwóch lub więcej sposobów uwierzytelniania klienta:

- coś co użytkownik wie (np. hasło)
- coś co użytkownik posiada (np. hasło sms)
- coś czym użytkownik jest (np. odcisk palca)

Standardy komunikacji bezpieczeństwa

Opinia Europejskiego Kongresu Finansowego w zakresie RTS dot. komunikacji konsultacji EBA

Sposób przeprowadzenia ankiety

Krok 1:
60 specjalistów zaproszonych do konsultacji

Krok 2:
EKF otrzymał odpowiedzi od 23 instytucji i ekspertów

Krok 3:
Seminarium zorganizowane przez EKF

Krok 4:
Zebranie i udokumentowanie wniosków przez EKF

Główne rekomendacje:

- Zasady silnego uwierzytelniania powinny pozostawiać dostawcom usług większą elastyczność co do sposobu realizacji uwierzytelniania. Na rynku polskim istnieją sprawdzone rozwiązania. Szczegółowe rekomendacje dot.:
  - Wprowadzenia wymogu logicznego powiązania urządzenia z użytkownikiem
  - Ograniczenia ryzyk w przypadku kradzieży urządzenia
  - Sprecyzowania zasad dot. generowania i przechowywania kodów autoryzujących
- Definicja dynamicznego powiązania urządzenia zawierającego parametry transakcji i inicjującego transakcję (art. 2.2 RTS) powinna być sprecyzowana. W szczególności powinna być możliwość pełnienia tych dwóch funkcji fizycznie przez jedno urządzenie mobilne (bądź przez odpowiednią definicję urządzeń powiązanych bądź przez dopuszczenie odpowiednich wyjątków).
- Zakres wyłączeń ze stosowania wymogów dot. bezpieczeństwa transakcji (uwierzytelnianie) powinien być bardziej dopasowany do faktycznych ryzyk (obecnych i przyszłych) oraz być powiązany z systemami oceny ryzyka nieautoryzowanej transakcji banków prowadzących rachunki płatnicze.

Standardy komunikacji bezpieczeństwa

Opinia Europejskiego Kongresu Finansowego w zakresie RTS dot. komunikacji konsultacji EBA

Sposób przeprowadzenia ankiety

Krok 1:
60 specjalistów zaproszonych do konsultacji

Krok 2:
EKF otrzymał odpowiedzi od 23 instytucji i ekspertów

Krok 3:
Seminarium zorganizowane przez EKF

Krok 4:
Zebranie i udokumentowanie wniosków przez EKF

Główne rekomendacje (cd.):

- Do RTS powinien zostać jasno wprowadzony zakaz przekazywania loginu i hasła do bankowości elektronicznej podmiotom trzecim przez użytkowników.
- Ogólnie otwarty standard komunikacji, w szczególności oparty o ISO 20022, byłby rozwiązaniem pożądanym. W praktyce jednak jest to problematyczne, gdyż obecnie wiele krajów ma lub opracowuje własne standardy i różnią się one istotnie.
- RTS powinien być uszczegółowiony w kwestiach dotyczących wskazania podmiotu finansującego koszt realizacji transakcji przez ASPSP jak również zasad odpowiedzialności PISP i AISP w przypadku błędów czy negatywnych zdarzeń.
- W odniesieniu do częstotliwości, z którą AISP miałby dostęp do informacji o rachunku bez każdorazowej inicjacji przez użytkownika, zdania ekspertów były podzielone. Ostatecznie EKF zarekomendował w ogóle rezygnację z dostępu bez inicjacji po stronie użytkownika – udział właściciela konta powinien być każdorazowo wymagany.

PSD2
Strategia biznesowa

Strategia biznesowa

Wpływ PSD2 na obecny model biznesowy banków

Przykładowe zagrożenia dla obecnych dochodów banków:

- Utrata dochodów z transakcji kartami
- Spadek dochodów z wymiany walut, wskutek dalszego uproszczenia procesu wymiany na niezależnych platformach walutowych
- Spadek dochodów z innych produktów, np. kredytów, depozytów – pośrednicy/agregatory ofert mogą kierować klienta do najkorzystniejszych cenowo miejsc
- Spadek roli banku jako punktu interakcji i wyboru usług tradycyjnie bankowych oraz spadek jakości relacji z klientem. Przeobrażenie się w dostarczyciela infrastruktury

Szanse

- Wykorzystanie API do dostarczenia nowych rozwiązań w zakresie płatności i wymiany walut
- Budowa szerszego ekosystemu usług wokół płatności, usług finansowych oraz identyfikacji/ potwierdzenia tożsamości
- Wzrost zysków dla podmiotów specjalizujących się w kredytach konsumpcyjnych z zaawansowaną analityką transakcyjną

Równolegle

- Pojawienie się alternatywnych rozwiązań i dostawców usług płatniczych, zarządzania finansami czy pożyczkodawców, np. przeobrażenie się mobilnych portmonetek czy dużych sieci handlowych w PISP
- Spadek cen dla punktów sprzedaży oraz klientów

Strategia biznesowa

Możliwe opcje strategiczne dla banków

Strategia dotycząca docelowego zakresu usług oraz miejsca w łańcuchu wartości określą decyzje banków dot. sposobu wdrożenia wymogów PSD2 w zakresie komunikacji:

Dla banków detalicznych wybór „wymaganego minimum” może oznaczać spadek przywiązania klientów.

Banki są postrzegane jako gwarantujące relatywnie większe bezpieczeństwo.

FinTechy koncentrują się na doświadczeniach klienta i ergonomii rozwiązania.

Strategia biznesowa

Przykłady wykorzystania PSD2 do rozwoju usług

- PFM – aplikacja (mobilna, on-line) do zarządzania finansami
- Agregator ofert/ doradca finansowy
- Szybkie metody płatności internetowych
- Zarządzanie płatnościami z różnych rachunków
- Scoring oparty na informacjach transakcyjnych
- Proces sprzedaży pożyczek oraz identyfikacji potrzeby kredytowej
- Platforma płatnicza dla firm
- Potwierdzanie tożsamości

Debata

PSD2 – realny wpływ nowej regulacji na kształt rynku bankowości detalicznej

Uczestnicy panelu

Piotr Alicki
Prezes Zarządu KIR

Maciej Biniek
Członek Zarządu
PayU

Mariusz Cholewa
Prezes Zarządu
Biuro Informacji Kredytowej

Tomasz Piwowarski
Dyrektor
Departament Inspekcji Bankowych, Instytucji Płatniczych i Spółdzielczych Kas Oszczędnościowo-Kredytowych
KNF

Paweł Wieczorek
b. Członek Zarządu
Bank Zachodni WBK

Kontakt

Dariusz Szkaradek
Partner
Lider Sektora Instytucji Finansowych
Deloitte

dszkaradek@deloittece.com

Deloitte.