Komisja
Nadzoru
Finansowego

Regulacyjne standardy techniczne i wytyczne EBA towarzyszące PSD2

Krzysztof Góral

Zastępca Dyrektora

Departament Inspekcji Bankowych, Instytucji Płatniczych i Spółdzielczych Kas Oszczędnościowo-Kredytowych

Urząd Komisji Nadzoru Finansowego

Warszawa, 23.05.2017 r.

Komisja Nadzoru Finansowego

Wybrane regulacje towarzyszące PSD2

- Regulacyjne standardy techniczne (RTS) dotyczące bezpiecznej komunikacji i silnego uwierzytelnienia

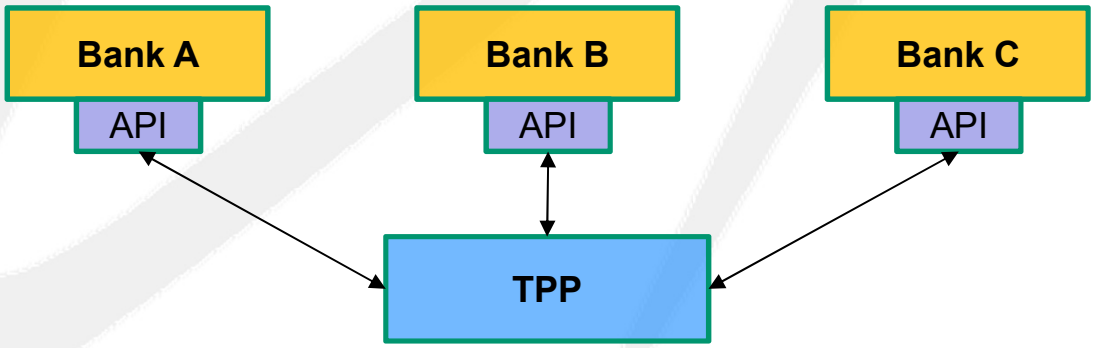
- Wytyczne dotyczące ryzyka operacyjnego i bezpieczeństwa w zakresie usług płatniczych

Komisja Nadzoru Finansowego

Regulacyjne standardy techniczne dot. bezpiecznej komunikacji i silnego uwierzytelnienia - projekt

Nowe interfejsy dostępu do rachunku płatniczego - API

Zgodnie z projektem RTS każdy dostawca usług płatniczych prowadzący rachunki płatnicze w trybie online będzie zobowiązany zbudować specjalny interfejs komunikacji z TPP (tzw. **API**) zapewniający możliwość pozyskiwania informacji o rachunku klienta lub zainicjowania transakcji.



Komisja Nadzoru Finansowego

Regulacyjne standardy techniczne dot. bezpiecznej komunikacji i silnego uwierzytelnienia - projekt

Stosowanie silnego uwierzytelnienia klienta

Zgodnie z art. 97 ust. 1 PSD2 dostawcy usług płatniczych powinni stosować silne uwierzytelnienie klienta w przypadku gdy płatnik:

a) uzyskuje dostęp do swojego rachunku płatniczego w trybie online;

b) inicjuje elektroniczną transakcję płatniczą;

c) przeprowadza czynność za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć.

Wyjątki od tej zasady będą określone w regulacyjnych standardach technicznych dotyczących bezpiecznej komunikacji i silnego uwierzytelniania.

Komisja Nadzoru Finansowego

Regulacyjne standardy techniczne dot. bezpiecznej komunikacji i silnego uwierzytelnienia - projekt

Wyłączenia w zakresie silnego uwierzytelnienia

1) Dostęp do informacji o rachunku bez ujawniania danych wrażliwych
2) Płatności zbliżeniowe (limity 50/150 EUR lub 5 kolejnych transakcji)
3) Płatności za transport i parkingi
4) Przelewy do zaufanych beneficjentów na tzw. białych listach
5) Przelewy powtarzalne (stała kwota i odbiorca płatności)
6) Przelewy wewnętrzne między rachunkami należącymi do jednego właściciela
7) Transakcje zdalne niskokwotowe (limity 30/100 EUR lub 5 kolejnych transakcji)
8) Transakcje zdalne w oparciu o analizę ryzyka (TRA) (limity od 100 do 500 EUR w zależności od stopy fraudów liczonej dla danego typu transakcji w ujęciu kwartalnym)

Komisja Nadzoru Finansowego

Regulacyjne standardy techniczne dot. bezpiecznej komunikacji i silnego uwierzytelnienia - projekt

Silne uwierzytelnienie klienta – wyłączenia w zakresie logowania do konta bankowego

Dostęp do historii transakcji za okres ostatnich 90 dni bez ujawniania danych wrażliwych nie wymaga stosowania silnego uwierzytelnienia klienta pod warunkiem, że:

1) Logowanie do rachunku nie jest wykonywane po raz pierwszy;

2) Logowanie do rachunku z zastosowaniem silnego uwierzytelnienia odbyło się w przeciągu ostatnich 90 dni.

Komisja Nadzoru Finansowego

Wytyczne dot. ryzyka operacyjnego i bezpieczeństwa w zakresie usług płatniczych - projekt

Główne obszary:

- Ramy zarządzania ryzykiem operacyjnym, bezpieczeństwem i outsourcingiem
- Ocena ryzyka, w tym identyfikacja kluczowych funkcji, procesów i zasobów
- Ochrona integralności oraz poufności danych i systemów
- Bezpieczeństwo fizyczne i kontrola dostępu
- Bieżące wykrywanie i monitorowanie zagrożeń
- Monitorowanie i raportowanie incydentów bezpieczeństwa
- Zarządzanie ciągłością działania i komunikacja w sytuacjach kryzysowych
- Świadomość sytuacyjna i ciągłe rozwijanie kompetencji
- Zarządzenie relacjami z użytkownikiem usług płatniczych

Komisja
Nadzoru
Finansowego

Dziękuję za uwagę