apilogic

Odszyfruj RTS

Regulatory Technical Standards do Dyrektywy PSD2 (w pigułce)

Przygotuj się do bankowości 4.0

Wejście w życie każdej unijnej dyrektywy finansowej nie jest procesem ani prostym, ani szybkim. To mozolna praca wielu jednostek organizacyjnych, skupiona na dostosowaniu prawa w taki sposób, by wszystkie zainteresowane grupy miały czas zgłosić swoje uwagi i poprawki.
Samo ogłoszenie tak ważnej dla całego rynku bankowości i płatności Dyrektywy PSD2 zaledwie rozpoczyna mozolny proces włączania w życie jej postanowień.

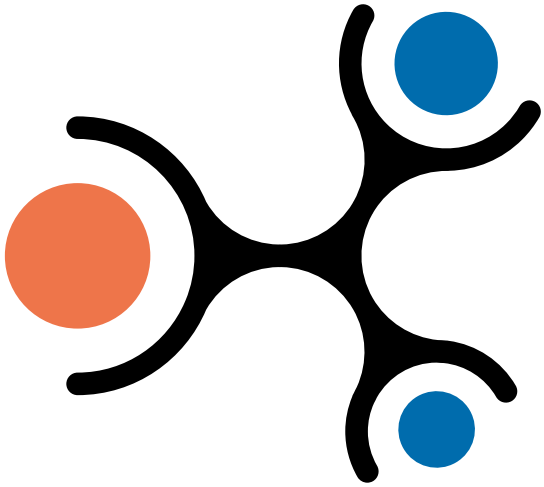
Aby rządy poszczególnych Państw członkowskich znały szczegółowe wskazówki, dzięki którym będą mogły dostosować lokalne prawo, organy nadzoru UE przygotowują dokument **RTS – Regulatory Technical Standards**, czyli tzw. „technikalia" do ustawy. Opisują one konkretne przypadki i dają wyjaśnienia dla stosowania tych,
a nie innych narzędzi dla zgodności z ustawą.

Wraz z zespołem konsultantów APILOGIC, przygotowaliśmy **standardy techniczne Dyrektywy PSD2 w formie skróconej**, rozumiejąc specyfikę językową i strukturalną dokumentów unijnych. Mamy nadzieję, że nasza publikacja będzie łatwiejsza do przyswojenia, dzięki czemu przyspieszycie Państwo wprowadzanie wytycznych ustawy w swoich organizacjach.

Życzę Państwu owocnej lektury!

Marcin Parczewski,
CEO Inteca i autor rozwiązania APILOGIC

Spis treści



Czym są RTS?

Dyrektywa jest narzędziem legislacyjnym Unii Europejskiej, którego głównym zadaniem jest nakreślenie celów i ogólnych warunków zmiany. Dostosowanie prawa w państwach członkowskich odbywa się już w oparciu o uwarunkowania lokalne, okoliczności prawne właściwe dla danego kraju.

Pomagają w tym **RTS**, czyli **standardy techniczne dla dyrektywy**.

Jak wygląda proces regulacji w usługach finansowych?

W prawodawstwie unijnym stosuje się tzw. podejście Lamfalussy'ego, umożliwiające elastyczny proces decyzyjny. Obejmuje ono cztery poziomy instytucjonalne:

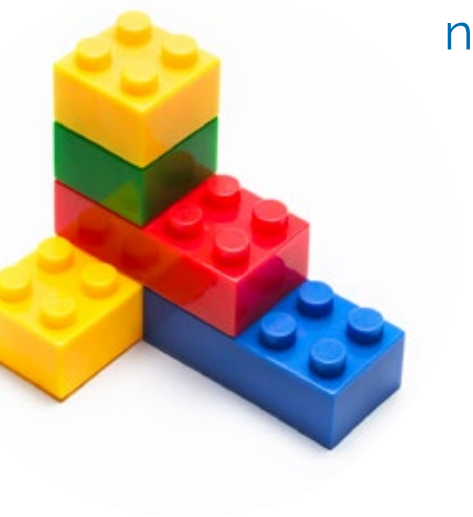
Poziom 1
W celu określenia zasad ramowych, Parlament Europejski i Rada przyjmują podstawowe prawa zaproponowane przez Komisję.

Poziom 2
Komisja może przyjąć, dostosować i zaktualizować techniczne środki wykonawcze przy pomocy organów konsultacyjnych złożonych z przedstawicieli krajów UE.

Poziom 3
Komitety krajowych organów nadzoru są odpowiedzialne za doradzanie Komisji w przyjmowaniu aktów poziomu 1 i 2 oraz wydawanie wytycznych dotyczących wdrażania przepisów.

Poziom 4
Komisja czuwa nad prawidłowym egzekwowaniem przepisów UE przez rządy krajowe.

Europejskie organy nadzoru (ESA)



Kompetencje tych organów obejmują odpowiedzialność za przygotowanie „standardów technicznych" - RTS, konkretnej kategorii środków poziomu 2, którą opracowują i przedstawiają Komisji.

- Europejski Organ Nadzoru Bankowego (EBA)
- Europejski Organ Nadzoru Giełd i Papierów Wartościowych (ESMA)
- Europejski Organ Nadzoru Ubezpieczeń i Pracowniczych
- Programów Emerytalnych (EIOPA)

środki poziomu 2

Wiele rozporządzeń i dyrektyw poziomu 1 w dziedzinie usług finansowych (zwanych „aktami podstawowymi") zawiera uprawnienia dotyczące środków poziomu 2, które mają zostać przyjęte przez Komisję w drodze aktów delegowanych, aktów wykonawczych lub środków przewidzianych w poprzedniej procedurze komitetowej „ Z kontrolą „. Środki te są zatwierdzone zgodnie z różnymi procedurami określonymi w odpowiednim akcie podstawowym i mogą podlegać formalnym decyzjom komitetu lub przewidywać niektóre prawa kontrolne Parlamentu Europejskiego i Rady.

Traktat lizboński, który wszedł w życie w 2009 r., stworzył obecny system aktów delegowanych i wykonawczych. Akty delegowane, o których mowa w art. 290 Traktatu, stanowią akty uzupełniające lub zmieniające niektóre, inne niż istotne, elementy aktu podstawowego.

Akty wykonawcze, o których mowa w art. 291, są stosowane, jeżeli wymagane są jednolite warunki wprowadzania |w życie aktów podstawowych.

W przypadku, gdy środki poziomu 2 wymagają ekspertyzy ekspertów nadzorczych, w podstawowym akcie można określić, że te środki są standardami technicznymi opartymi na projektach opracowanych przez europejskie organy nadzoru.

W grupie środków poziomu 2 są obecne dwa typy standardów:

- **Regulacyjne standardy techniczne (RTS), (przyjmowane przez Komisję w drodze aktu delegowanego)**
- Wykonawcze standardy techniczne (ITS) (przyjmowane w drodze aktu wykonawczego)

RTS – finalny projekt standardów technicznych

Projekt oznacza, że wciąż czekamy na ostateczny kształt wytycznych RTS. Zostaną (najprawdopodobniej jeszcze w 2018 roku) przedstawione do akceptacji Komisji Europejskiej, następnie zbadane przez Parlament Europejski i opublikowane w oficjalnym Dzienniku Ustaw Unii Europejskiej. 20 dni później Regulacja zyska moc prawną.

Final Draft on Regulatory Technical Standards

Postanowienia ogólne

Operatorzy płatności PSP muszą wykorzystywać **mechanizmy monitorujące transakcje**, które podczas analizy typowych zachowań użytkownika dokonującego transakcji, automatycznie wykrywają próby oszustwa, używając **zestawów reguł**.

Jakie elementy ryzyka transakcji muszą zawierać zestawy?

wszelkie brakujące lub złamane elementy uwierzytelniające

kwota każdej transakcji

znane scenariusze oszustw

symptomy obecności złośliwego oprogramowania

Jeśli operator płatności PISP zrezygnował z silnego uwierzytelniania SCA powinien nadzorować takie elementy, jak:

- ścieżki transakcyjne
- historia operacji (u różnych operatorów)
- lokalizacja użytkownika
- lokalizacja urządzenia dostępowego
- lokalizacja oprogramowania
- anomalie w ścieżkach trans-akcyjnych (w relacji do historii transakcji)
- czas logowania do urządzenia lub oprogramowania
- nietypowe użycie urządzenia lub oprogramowania

obowiązkowe audyty

Raz w roku operator ma obowiązek przeprowadzić audyt skuteczności mechanizmów i ich **zgodności z aktualną wersją Regulacji**. Wyniki audytu muszą być stale dostępne do wglądu organów kontrolnych.

PATRZ W PRZYSZŁOŚĆ

ODKRYWAJ. ROZWIJAJ. WYPRZEDZAJ.

Skontaktuj się z nami i umów prezentację.

apilogic

Otwarte API Bankowe

Apilogic jest gotowym rozwiązaniem, które pomoże szybciej osiągnąć zgodność z Dyrektywą PSD2 i Standardami Otwartej Bankowości. Apilogic to najwyższej klasy komponenty technologiczne, które możesz nałożyć na dowolną infrastrukturę.

Umów się na prezentację i uzyskaj więcej informacji jeszcze dzisiaj.

apilogic.pro

Środki bezpieczeństwa w ramach Silnego Uwierzytelniania Klienta (SCA)

Dyrektywa PSD2 nakłada na wszystkie zaangażowane podmioty obowiązek **Silnego Uwierzytelniania Klienta** (SCA – ang. Strong Customer Authentication), co w praktyce oznacza 3-składnikową weryfikację transakcji i jej inicjatora.

PSD2: weryfikacja 3-stopniowa

Co dokładnie oznacza Silne Uwierzytelnienie Klienta (SCA)?

something the user have

Coś, co użytkownik posiada, np. telefon komórkowy lub elektroniczny token. Operatorzy płatności PISP muszą zweryfikować, czy nie został przejęty przez osoby nieupoważnione. Pod uwagę należy wziąć również możliwość skopiowania urządzenia czy jego oprogramowania.

something the user is

Odcisk palca, szablon głosu czy skan tęczówki użytkownika to niemożliwe do skopiowania elementy, klasyfikowane jako coś, czym użytkownik jest. Dostawcy usług płatniczych TPP powinni zapewnić narzędzia biometryczne weryfikujące, że nikt nie podszył się pod użytkownika.

something the user knows

Element określony jako wiedza (np. kod PIN, hasło dostępu). Operatorzy płatności PSP muszą podjąć szczególne środki ostrożności, by utajnić ten element podczas procesu weryfikacji.

Kiedy mamy do czynienia z Silnym Uwierzytelnieniem Klienta, po weryfikacji powinno nastąpić wygenerowanie tokenu - kodu dostępu, który może być użyty do sprawdzenia konta, przeprowadzenia płatności elektronicznej lub każdej innej zdalnej czynności, stanowiącej ryzyko oszustwa czy wyłudzenia.

Kod dostępu

Sugerowane środki bezpieczeństwa:

- ✗ kod dostępu nie powiązany z elementami SCAQ
- ✗ brak powiązań kodów z poprzednio wygenerowanymi
- ✗ uniemożliwienie sfałszowania kodu

ważne!

W przypadku, gdy kod nie mógł zostać wygenerowany **przez niespełnienie podstawowych wymogów bezpieczeństwa**, w ramach Silnego Uwierzytelniania Klienta muszą zostać poprawnie **zweryfikowane wszystkie 3 składniki**. Komunikacja w ramach autoryzacji powinna być zabezpieczona przed podglądem i dostępem podmiotów nieupoważnionych.

Blokada

Po 5 nieudanych próbach autoryzacji, narzędzie płatnicze powinno zostać tymczasowo lub permanentnie zablokowane, a ilość prób przed całkowitą blokadą będzie zależna od charakteru operacji i uwzględnionego w nim ryzyka.

⚠ Użytkownik powinien być wyraźnie ostrzeżony przed całkowitą blokadą!

Co zrobić, kiedy blokada jest już nałożona?

Należy udostępnić możliwość wystąpienia o ponowny dostęp do narzędzi płatniczych, w ramach ustanowionej procedury bezpieczeństwa.

Podstawowe środki bezpieczeństwa dla PSP

- informowanie użytkownika o dostawcy i kwocie transakcji
- generowanie jednorazowego kodu dostępu
- zasada: jedna transakcja, jeden kod
- zmiana kwoty transakcji: nowy kod

indywidualny kod transakcji musi zawierać:
- **sumę płatności w transakcji**
- **dobrze zdefiniowanego odbiorcę**

Płatności okresowe

Stałe polecenia przelewu, gdy dokonywane na rzecz różnych podmiotów,

wtedy

ważne!

Elementy **Silnego Uwierzytelnienia Klienta** (SCA) powinny być od siebie niezależne, sprawdzane za pomocą środków bezpieczeństwa dla zagwarantowania ich odrębności i stanu, w którym **złamanie lub naruszenie jednego z elementów nie wpływa na pozostałe**.

Gdy uwierzytelniamy z pomocą urządzenia mobilnego:

- PSP powinien dodatkowo wzmocnić środki bezpieczeństwa, by zminimalizować ryzyko nadużycia
- oprogramowanie urządzenia powinno mieć osobne środowiska dla różnych stopni weryfikacji
- każde ryzyko zmian w urządzeniu powinno być monitorowane przez odpowiednie mechanizmy

Wyjątki stosowania Silnego Uwierzytelnienia Klienta (SCA)

Należy pamiętać o tym, że obciążające sieć mechanizmy uwierzytelniające nie zawsze są konieczne. **Dobro i komfort użytkownika ma również swój priorytet**. Regulator dopuścił wiele wyjątków od obowiązku 3-stopniowej weryfikacji.

Kiedy PSP może zostać zwolniony z obowiązku Silnego Uwierzytelniania?

- przy sprawdzaniu stanu konta bankowego,
- i/lub kiedy wykonuje transakcje płatnicze w czasie do 90 dni od ostatniego SCA

Wyjątki nie mają zastosowania, gdy:

- powyższych operacji klient dokonuje po raz pierwszy
- Silne Uwierzytelnienie było przeprowadzone ponad 90 dni wstecz
- transakcja jest zbliżeniowa, na kwotę do 50 euro
- od ostatniego SCA nie przekraczają: 5 kolejnych transakcji & 150 Euro
- dotyczy płatności za:
  - parking w terminalach parkingowych
  - bilety w terminalach transportowy

Kiedy jeszcze podczas transakcji nie stosujemy Silnego Uwierzytelniania?

- gdy odbiorca znajduje się w bazie zapisanych przez użytkownika kontaktów
- zostało wyznaczonych kilka transakcji na tę samą kwotę do tego samego odbiorcy
- gdy użytkownik wykonuje przelewy własne w ramach tego samego konta

Analiza ryzyka transakcyjnego

W ramach dokonywanych transakcji, spełniających wymogi Silnego Uwierzytelnienia, operatorzy płatności są zwolnieni z wymogów silnego uwierzytelnienia, gdy **klient zapoczątkowuje transakcję zdalną i jest ona zakwalifikowana jako mało ryzykowna** przez mechanizmy bezpieczeństwa.

Czynniki ryzyka, brane pod uwagę przez mechanizmy:

- kwoty progowe wyłączenia dodatkowych zabezpieczeń transakcji (SCA), w zależności od ich wysokości oraz sposobu zawierania transakcji (karta, płatność elektroniczna). Limity są zawarte w poniższej tabeli:

	Reference Fraud Rate (%) for:	
ETV	Remote card-based payments	Credit transfers
EUR 500	0.01	0.005
EUR 250	0.06	0.01
EUR 100	0.13	0.015

- dane o transakcji muszą być poddane automatycznej analizie w czasie rzeczywistym i na podstawie zestawów reguł przypisane do danego poziomu ryzyka. **Transakcja z wyłączeniem SCA nie może przekraczać 500 EUR.**

Kiedy PSP jest zwolniony z SCA?

- gdy kwota transakcji nie przekracza 30 Euro
- suma kwot (maksymalnie 5) transakcji nie przekracza 100 Euro
- mechanizmy ryzyka ocenią płatność jako mało ryzykowną

Co wpływa na ocenę mechanizmów ryzyka?

- nie zostało wykryte nietypowe zachowanie czy lokalizacja użytkownika
- nie pojawiły się odstające od normy informacje
- nie zostało wykryte zagrożenie złośliwym oprogramowaniem
- nie zostały wykryte scenariusze wyłudzeń

Obowiązkiem operatorów płatności PSP jest monitorowanie następujących danych*:

(gdy rezygnują z Silnego Uwierzytelniania)

- całkowita wartość transakcji nieautoryzowanych
- całkowita wartość wszystkich transakcji wraz ze współczynnikiem oszustw
- średnia wartość transakcji, z podziałem na dokonywane z SCA i z wyłączeniem SCA
- ilość transakcji nieautoryzowanych, wraz z danymi o całkowitej liczbie transakcji

* **dane muszą być przechowywane i dostępne do wglądu dla upoważnionych organów kontrolnych**

W przypadku, gdy PSP nie spełnia tych wymogów:

- zostaje zablokowana możliwość wyłączenia SCA dla dokonywanych transakcji
- ma możliwość odblokowania po spełnieniu wszystkich warunków
- odblokowanie nastąpi pod warunkiem przesłania raportu do organów kontrolnych

ważne!

Jeśli kontrole wykażą, że zagrożenie oszustwem bądź wyłudzeniem wzrosło dla tego PSP, mogą wymagać Silnego Uwierzytelniania nawet w przypadkach, gdzie wcześniej było stosowane wyłączenie.

Poufność i integralność danych osobowych użytkowników

Zarządzanie pieniędzmi niesie ze sobą kwestie bezpieczeństwa, również danych biorących udział w transakcji. Muszą być one silnie chronione i Standardy Techniczne dla nowej dyrektywy określają, jakie są elementy tej ochrony. **Niektóre z dotychczas stosowanych (np. hasła SMS) nie będą już zgodne z PSD2.**

Jakie szczególne środki ochrony danych musi stosować PSP?

Dane osobowe u operatora PISP:

- pełna dokumentacja procesu ochrony danych
- wzmocnione zabezpieczenie danych w obiegu
- ograniczenie nieuprawnionego dostępu do uczestniczących w weryfikacji:
  - danych osobowych
  - urządzeń
  - oprogramowania

podczas procesu weryfikacyjnego tylko część danych jest widoczna

dane bezpieczeństwa nie są przechowywane w formie tekstowej

dane są odpowiednio zabezpieczone przed nieuprawnionym dostępem

ważne!

PSP musi mieć pewność, że dane osobowe, urządzenie i oprogramowanie są bezpiecznie przypisane do i wykorzystywane tylko przez jednego użytkownika. W szczególności należy zabezpieczyć proces połączenia tych elementów w procesie zdalnym – obowiązuje wtedy **zasada Silnego Uwierzytelnienia**

Rezygnacja z zabezpieczeń na ryzyko operatora płatności (PSP)

jest objęta obowiązkami prowadzenia statystyki kwartalnej, dotyczącej:

- ilości transakcji nie objętych weryfikacją
- łącznej sumy tych transakcji
- wszystkich zarejestrowanych wtedy przypadków nadużyć

Podsumowanie

Dyrektywa PSD2 wkracza, kiedy rynek nowoczesnych usług finansowych jest już na tyle rozwinięty, że pojawiła się potrzeba **uregulowania i uporządkowania** kwestii związanych z nimi. Głównie w trosce o **bezpieczeństwo i komfort użytkownika**. Chociaż **standardy techniczne** mogą się jeszcze nieznacznie zmienić, zawarty w nich przekaz pozostanie ten sam – infrastruktura banku **musi zostać otwarta**. Nie bez znaczenia pozostaje czas, potrzebny na **wdrożenie API i innych technologicznych rozwiązań**, nakazywanych ustawą. Dlatego nie warto czekać i już dzisiaj **rozpocząć transformację**. Potężna ustawa, jaką jest **dyrektywa PSD2**, ma na celu **pobudzenie rynku**. W ekonomicznym wyścigu zwycięży ten, kto w porę zajmie dobre miejsce.


BĄDŹ LIDEREM INNOWACJI
ODKRYJ MOC TWOICH DANYCH!
Dowiedz się więcej o APILOGIC
Apilogic pomaga łatwo zintegrować Twoje systemy z siecią zewnętrznych dostawców. Skorzystaj z doświadczenia naszych inżynierów i sprawnie przeprowadź swój bank przez cyfrową transformację. Umów się na prezentację i uzyskaj więcej informacji jeszcze dzisiaj.
apilogic
apilogic.pro
Otwarte API Bankowe

Rozwiązujemy złożone problemy infrastruktury IT.

Wspieramy w zakresie:

- Architektur korporacyjnych
- Zarządzania procesami
- Budowy aplikacji biznesowych

Co jest dla nas najważniejsze?

Nacisk na wyniki

Najwyższą wartością, decydującą o powodzeniu projektu, jest dla nas wynik biznesowy w ujęciu zarówno zysków, jak i oszczędności i czasu wdrożenia.

Narzędzia

Starannie dobieramy elementy i zestawy oprogramowania w służbie doskonałych projektów i wysokiej jakości produktów informatycznych.

Zwinne metodyki

Pracujemy według metodyk zwinnych Agile i Scrum, proces wytwarzania oprogramowania wspieramy wypracowanym przez lata autorskim modelem MDE.

Doświadczenie

Uczestniczyliśmy w pionierskich projektach związanych z cyfrową ewolucją bankowości, od lat współpracujemy z bankami w zakresie technologii informatycznych.

Kultura relacji

Wierzymy w ogromną wartość dobrych relacji w biznesie i wysokich standardów obsługi klienta. Stoimy na straży efektywnej komunikacji projektowej.

Najlepsi partnerzy

Współpracujemy z wiodącymi światowymi dostawcami oprogramowania do modelowania procesów, projektowania, budowy czy integracji systemów.

Inteca | IT's about business

Dowiedz się więcej

ul. Kościuszki 14 | 50-038 Wrocław | biuro@inteca.pl | tel. +48 71 715 60 91