Z początkiem 2018 roku weszła w życie nowa dyrektywa unijna regulująca rynek płatności Payments Services Directive 2 (PSD2), która obejmuje swoim zasięgiem wszystkie kraje Unii Europejskiej. W związku ze zmianą norm prawnych, instytucje sektora finansowego powinny jak najszybciej dostosować swoją architekturę IT.

Nowe regulacje

Rozwój usług świadczonych drogą elektroniczną sprawił, że na rynku pojawiły się nowe rozwiązania, które do tej pory nie były uregulowane prawnie. Główne cele przyjętej przez Parlament Europejski w dniu 8 października 2015 r. dyrektywy PSD2 w sprawie usług płatniczych w ramach rynku wewnętrznego, to rozszerzenie ram prawnych określających zasady świadczenia usług płatniczych, uzupełnienie istniejących regulacji, a także wyjaśnienie powstałych na ich tle wątpliwości.

Postanowienia PSD2 mają znaczny wpływ na kształt całego rynku usług płatniczych, a tym samym na działalność banków, instytucji finansowych, oraz wszystkich innych podmiotów oferujących karty sklepowe czy karty paliwowe. Zmiany obejmują również innych dostawców usług płatniczych, zainteresowanych w szczególności rozwojem szeroko pojętych płatności mobilnych. Jednym z założeń dyrektywy jest umożliwienie dostępu osobom trzecim – Third Party Providers (TTP) do informacji o koncie klienta, jego historii transakcji oraz dokonywanie płatności w jego imieniu – oczywiście, o ile klient wyrazi na to zgodę.

Katalog usług płatniczych został rozszerzony o dwa nowe typy usług:

1. Payment Initiation Service (PIS)– usługę inicjowania płatności, która pozwala na udzielenie TPP dostępu do rachunków online klienta i realizowanie płatności w jego imieniu do określonego odbiorcy oraz raportowanie o dokonanej transakcji.
2. Account Information Service (AIS) – usługę dostępu do informacji o rachunku, która pozwala TPP na pobieranie informacji o rachunkach płatniczych klienta u jednego lub kilku dostawców, dzięki czemu klient za pośrednictwem TPP będzie mógł natychmiast uzyskać informacje o swojej sytuacji finansowej.

W związku z tymi zmianami, dostawcy usług płatniczych zobowiązani są do zapewnienia bezpiecznej, dwustronnej komunikacji pomiędzy urządzeniem płatnika, a urządzeniem wykorzystywanym do akceptacji płatności. Na przykład poprzez uniemożliwienie nieuprawnionego przekierowania płatności lub informacji.

Jak zagwarantować bezpieczeństwo?

W kontekście architektury IT należy zadbać o bezpieczny sposób udostępniania danych podmiotom zewnętrznym. W celu zachowania bezpiecznej komunikacji oraz monitorowania

udostępnianych usług, Regulacyjne Standardy Techniczne (RTS) narzucają na instytucje finansowe konieczność stworzenia dedykowanego interfejsu komunikacyjnego (API) oraz zastosowania mechanizmów silnego uwierzytelnienia – Strong Customer Authentication (SCA).

API – to sprawdzona technologia, która wykorzystuje dobrze znane techniki programowania i komunikacji. Najczęściej również nie wymaga zmian w infrastrukturze systemów. Interfejsy API zapewniają więc wygodną i stabilną komunikację. Mogą także uruchomić dodatkowe źródła przychodów, poprzez wprowadzenie nowych, wartościowych dla konsumenta usług. Znajdują zastosowanie w aplikacjach webowych, mobilnych, Service Oriented Architecture (SOA) oraz dla usług i aplikacji w chmurze.

SCA – ma zapewnić wyższy poziom wiarygodności poprzez uwierzytelnienie dwuczynnikowe, czyli oparte o zastosowanie co najmniej dwóch elementów z kategorii:
⇒ wiedza (coś, o czym wie tylko użytkownik np. dane logowania),
⇒ posiadanie (coś, co posiada wyłącznie użytkownik np. kod sms),
⇒ cechy klienta (coś, co charakteryzuje użytkownika).

Jak wybrać właściwe rozwiązanie ?

Większość banków oferujących usługę bankowości elektronicznej stosuje już mechanizmy silnego uwierzytelnienia, które można wykorzystać używając odpowiedniej technologii do wdrożenia warstwy interfejsów API. Instytucje finansowe udostępniając swoje usługi muszą zadbać o bezpieczeństwo. Należy zapewnić pełną kontrolę nad procesem rejestracji podmiotów trzecich. Istotny jest również monitoring usług API i nakładanie limitów na liczbę wywołań usługi czy możliwość wstrzymania lub anulowania dostępu w przypadku próby nadużyć. Ważne jest również odpowiednie przygotowanie dla partnerów dostępu do dokumentacji technicznej oraz środowiska testowego, w którym sprawdza się integracje z danym bankiem.
Z uwagi na dużą liczbę podmiotów trzecich, najlepszym rozwiązaniem jest dedykowany portal z dokumentacją techniczną API, który umożliwia automatyczną rejestrację nowych podmiotów oraz generowanie odpowiednich kodów dostępu i kluczy uwierzytelniających. Takie możliwości daje platforma CA PSD2 API.

Bezpieczeństwo, elastyczność i renoma

Platforma CA PSD2 API została zaprojektowana, aby sprostać wszystkim wyzwaniom sektora finansowego i zapewnić dodatkową warstwę nadzoru. Dzięki rozszerzeniu standardu CA API

Management o dedykowany dla sektora finansowego „add-on”, spełnia najwyższe standardy bezpieczeństwa i przyspiesza proces wdrożenia. Pozwala szybko agregować dane z różnych systemów i poprawić mobilność. Gwarantuje stabilność, umożliwia monitorowanie, raportowanie oraz rozliczanie udostępnianych usług.
Dla uzyskania maksymalnej elastyczności, CA API Management składa z trzech produktów, koncentrujących się na konkretnych obszarach cyklu życia API, które mogą być także dostarczone oddzielnie.
CA API Gateway
CA API Portal
CA Live API Creator
CA API Management umożliwia:
wykorzystanie istniejących i starszych już aplikacji poprzez adaptację protokołu w celu szybszego wprowadzania na rynek nowych rozwiązań,
dostarczanie nowych, najwyższej jakości usług za pomocą złożonych aplikacji,
bezpieczne zarządzanie zewnętrznymi interfejsami API,
rozszerzenie zasięgu rynkowego przedsiębiorstwa, dzięki udostępnieniu zewnętrznym deweloperom interfejsów API do systemów i danych firmy.
Rozwiązanie oferuje organizacjom innowacyjne możliwości w procesie tworzenia i zapewnienia maksymalnego bezpieczeństwa wytwarzanych aplikacji poprzez:
umożliwienie zarządzania pełnym cyklem życia API w procesie wytwórczym oprogramowania,
wprowadzenie dodatkowej warstwy zabezpieczeń na poziomie API dla aplikacji,
umożliwienie pełnej kontroli wymiany danych pomiędzy różnymi aplikacjami.
Pozycję systemu CA API Management, jako lidera w technologii API Management, potwierdzają najbardziej renomowane, niezależne firmy analityczno-doradcze, takie jak Gartner i Forrester Research. Rozwiązania firmy CA Technologies są oceniane jako najlepsze z dostępnych na rynku.
Mariusz Petrykowski

Business Development Director at Telsar Sp. z o.o.