



Praktyczny podręcznik po dyrektywie PSD2

Płatności internetowe



Spis treści

Wprowadzenie	3
Silne uwierzytelnianie	4
Elementy uwierzytelniania	4
Okres wdrożenia	4
Silna autentykacja EMV	5
Korzyści z aktualizacji do najnowszej wersji silnej autentykacji zgodnej ze standardem EMV	5
Przeniesienie odpowiedzialności	5
Jak to działa	6
Co to oznacza dla Państwa klientów?	7
Co to oznacza dla sprzedawców?	7
W jaki sposób Elavon może pomóc?	7

Wprowadzenie

Dyrektywa w sprawie usług płatniczych 2 (PSD2) to dyrektywa wydana przez Komisję Europejską, która zobowiązuje do stosowania silnego uwierzytelniania (SCA) we wszystkich transakcjach obejmujących płatności internetowe.

Od 2017 roku do końca 2018 roku straty poniesione przez firmy w Wielkiej Brytanii na skutek oszustw z wykorzystaniem kart płatniczych wzrosły o 19%, generując koszty na poziomie 760 mln euro¹. Dyrektywa PSD2, której celem jest ograniczenie oszustw płatniczych, wprowadza obejmujące całą branżę zmiany zwiększające bezpieczeństwo klientów i firm w całej Unii Europejskiej.

- Dyrektywa obejmie wszystkie przedsiębiorstwa akceptujące płatności kartowe zarejestrowane lub obsługujące klientów w Europejskim Obszarze Gospodarczym.
- Nowe przepisy wprowadzają mechanizmy bezpieczeństwa zwane uwierzytelnianiem dwuskładnikowym, których celem jest zapewnienie bezpieczeństwa klientom realizującym płatności internetowe. Zmiana ta obejmuje całą branżę.
- Przedsiębiorstwa muszą zaktualizować infrastrukturę płatniczą, tak aby zapewnić obsługę uwierzytelniania dwuskładnikowego. Dzięki temu wszystkie podmioty w ekosystemie będą miały dostęp do dokładniejszych danych, przez co będą mogły podejmować skuteczniejsze decyzje w zakresie autoryzacji płatności.
- Rozwiązania w zakresie silnego uwierzytelniania oferowane przez Elavon wykorzystują najnowszą technologię pozwalającą na analizę ryzyka z czasie rzeczywistym, która nie zakłóca procesu płatności realizowanego przez klientów.
- Zwiększony poziom bezpieczeństwa i kontroli przyniesie bezpośrednie korzyści klientom oraz zwiększy ich zaufanie do zakupów internetowych.



**Oszustwa
związane z kartami
kosztowały firmy
760 mln euro
w 2018 r.¹**

1. [statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/](https://www.statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/)



Silne uwierzytelnianie

Silne uwierzytelnianie oznacza, że przed zatwierdzeniem transakcji banki muszą potwierdzić, że użytkownik karty jest jej faktycznym właścicielem.

Użytkownik karty, aby udowodnić, że jest faktycznym właścicielem, musi wykonać uwierzytelnienie, podając co najmniej dwa z trzech elementów wymaganych przez bank.

Elementy uwierzytelniania

Uwierzytelnianie obejmuje dowolną kombinację dwóch z poniższych elementów:

Wiedza – oznacza coś, co wie wyłącznie użytkownik i bank.

Podawanie hasła lub innych ważnych informacji jest metodą dotychczas stosowaną w branży, która spełnia ten wymóg.



Posiadanie – coś, co posiada wyłącznie użytkownik karty i może być rozpoznane przez bank.

Token lub telefon automatycznie spełnia ten wymóg.



Cecha – coś, co jest unikalne dla użytkownika karty i możliwe do zweryfikowania przez bank.

Odcisk palca, rozpoznawanie twarzy i głosu lub skan siatkówki oka są przykładami zabezpieczeń, których popularność będzie rosła w miarę rozwoju i dojrzewania technologii.



Okres wdrożenia

Europejski Urząd Nadzoru Bankowego dostrzegł złożoność i trudności związane z wdrożeniem tej dyrektywy w środowisku płatniczym i wydłużył wyznaczony na to pierwotnie okres. Nowym terminem na uzyskanie zgodności z dyrektywą w branży płatności internetowych w Europie jest 31 grudnia 2020 r.

W Wielkiej Brytanii termin wyznaczony przez Finansowy Urząd Nadzorczy jest dłuższy i kończy się 31 marca 2021 r.

Ten dodatkowy czas jest niezbędny, aby zapewnić, że wszystkie podmioty działające w ekosystemie, banki, agenci rozliczeniowi oraz sprzedawcy nabędą odpowiednie narzędzia służące pełnemu wdrożeniu dyrektywy PSD2. Podmioty te muszą przeprowadzić wdrożenie terminowo, a także powinny dążyć do minimalizacji wpływu prac na klientów.

Sprzedawcy muszą w pełni wykorzystać okres migracji. W dalszym ciągu należy prowadzić prace z dostawcami rozwiązań, aby zapewnić wdrożenie protokołów silnej autentykacji opartych o branżowy standard EMV, które umożliwiają bankom przeprowadzanie dwuskładnikowego uwierzytelniania klientów.

Nowym terminem na uzyskanie zgodności z dyrektywą w branży płatności internetowych w Europie jest 31 grudnia 2020 r.



Silna autentykacja EMV

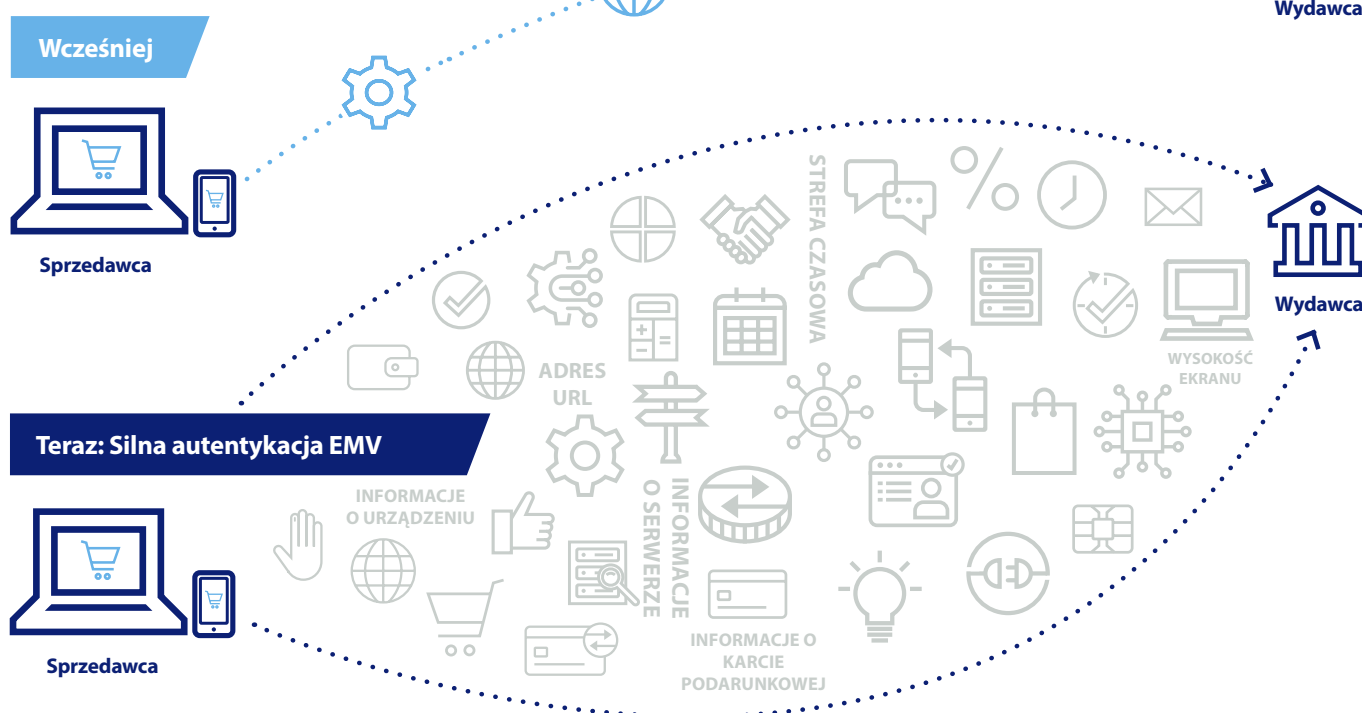
Silna autentykacja EMV jest standardowym protokołem stosowanym do silnego uwierzytelniania podczas akceptowania płatności w internecie. Pozwala ograniczyć liczbę oszustw oraz rezygnacji z finalizacji zamówień, a jednocześnie umożliwia sprawne zintegrowanie dodatkowych danych z istniejącymi informacjami.

Aktualizacja do ostatniej wersji zabezpieczeń pozwoli sprzedawcom na większą elastyczność działania. Kolejną korzyścią stosowania silnej autentykacji EMV jest przeniesienie odpowiedzialności na dostawców usług płatniczych.

Silna autentykacja EMV	2.1	2.2
Silne uwierzytelnianie dla połączonych urządzeń i zakupów internetowych	✓	✓
Scenariusze uwierzytelnienia w środowisku pozapłatniczym, np. poprzez dodanie kart płatniczych do aplikacji sprzedawcy	✓	✓
Wsparcie dla wszystkich dostępnych typów wyłączeń silnego uwierzytelnienia		✓
Typowe dla Europy scenariusze zgodne z dyrektywą PSD2, np. zaufany odbiorca i uwierzytelnianie delegowane		✓
Wykorzystanie danych biometrycznych konsumentów		✓

Zalecamy rozpoczęcie przygotowań do uwierzytelniania poprzez wdrożenie najnowszej wersji silnej autentykacji zgodnej ze standardem bezpieczeństwa EMV. Warto skontaktować się z dostawcą usług bramki płatniczej w celu omówienia migracji do najnowszej wersji silnej autentykacji EMV, która stanie się szeroko dostępna w 2020 r.

Dzięki tej aktualizacji będą mogli Państwo skorzystać z maksymalnego dopuszczonego zakresu typów wyłączeń wdrożonych na Państwa rynku.



Korzyści z aktualizacji do najnowszej wersji silnej autentykacji zgodnej ze standardem EMV

- Większe zaufanie użytkowników kart podczas zakupów w Państwa firmie
- Mniejsza liczba oszustw i reklamacji chargeback – ochrona przed odpowiedzialnością
- Zapobieganie transakcjom odrzucanym przez brak uwierzytelnienia
- Trafniejsze decyzje podejmowane na podstawie oceny ryzyka generujące większą liczbę zatwierdzanych płatności
- Pełne wsparcie dla wszystkich dostępnych typów wyłączeń oraz typów urządzeń płatniczych

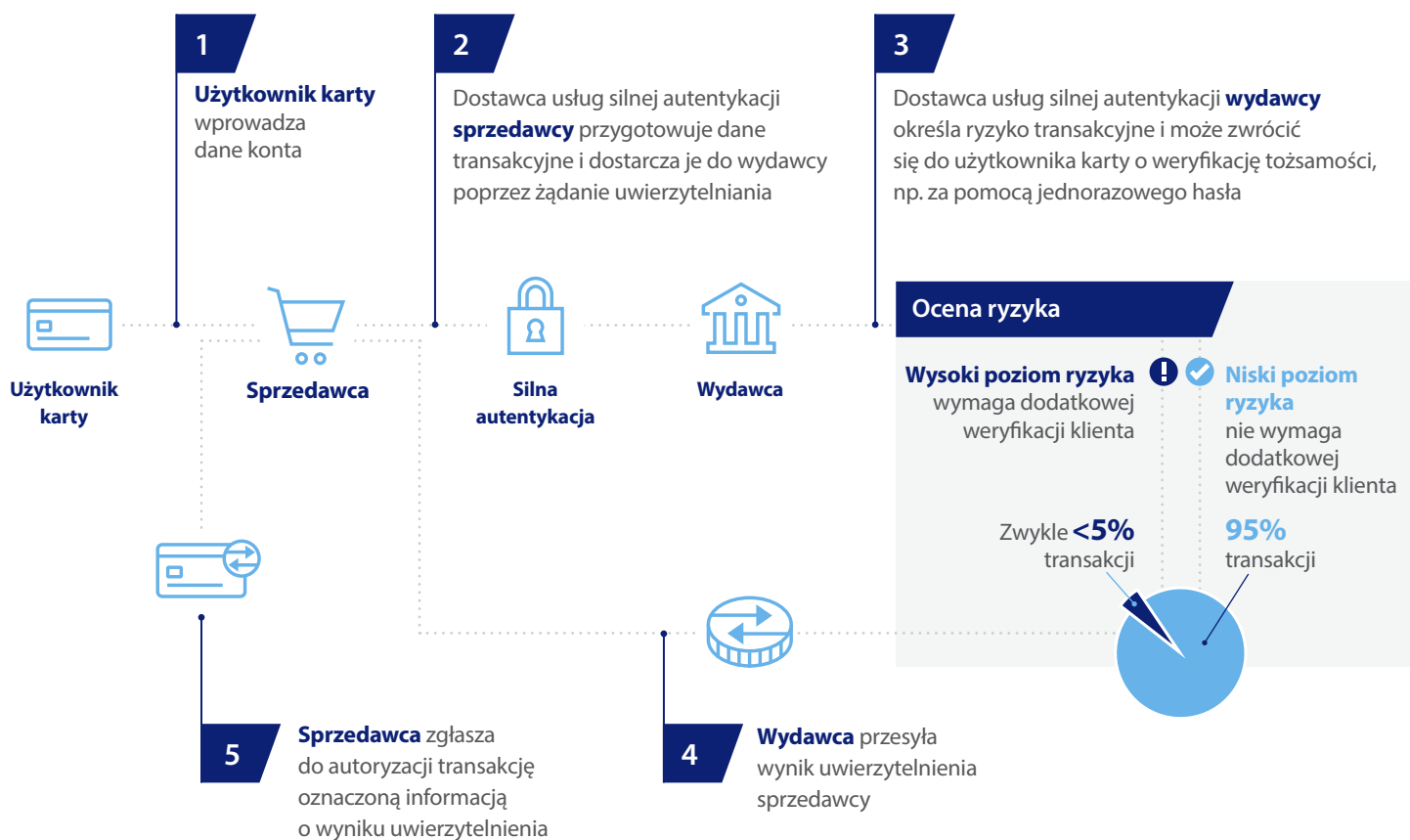
Przeniesienie odpowiedzialności

Po wdrożeniu procesu uwierzytelniania silnej autentykacji EMV (o ile data przeniesienia odpowiedzialności weszła już w życie w Państwa regionie) ryzyko wystąpienia reklamacji chargeback w Państwa firmie będzie minimalne.

Daty wdrożenia przeniesienia odpowiedzialności różnią się w zależności od sieci i regionu geograficznego. Informacje dotyczące dat obowiązujących w Państwa regionie można uzyskać u dostawcy usług bramki płatniczej.

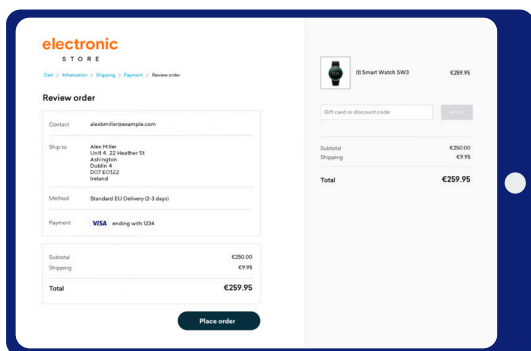


Jak to działa

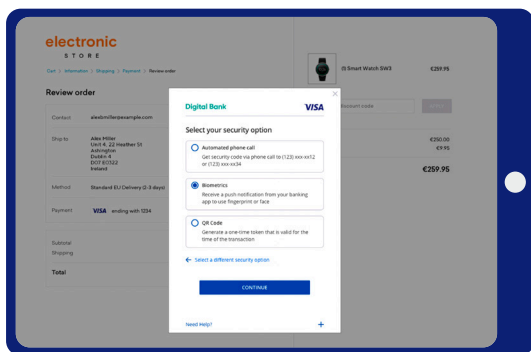


Co to oznacza dla Państwa klientów?

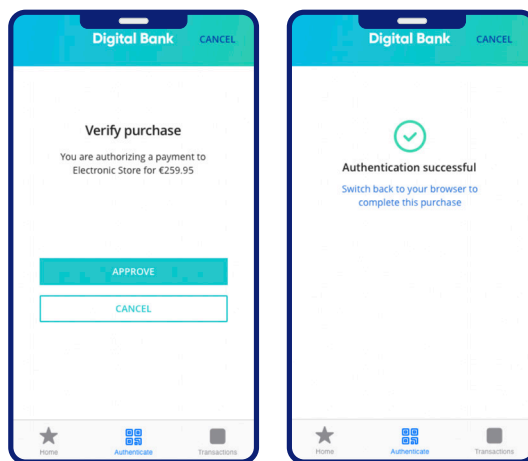
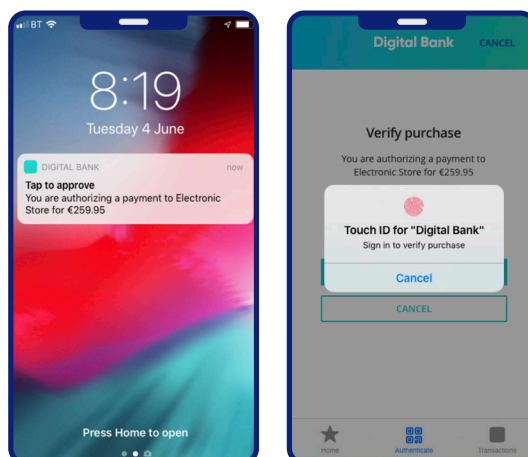
1. Klient zamierza wykonać płatność elektroniczną za pomocą komputera, laptopa, telefonu komórkowego lub innego urządzenia i przechodzi to strony płatności.



2. Aby zakończyć transakcję, klient wybiera sposób uwierzytelnienia lub postępuje zgodnie z metodą wybraną przez wydawcę swojej karty.



3. W celu realizacji płatności klient musi postępować zgodnie z instrukcjami.



Co to oznacza dla sprzedawców?

Nowe reguły będą oznaczać, że większość transakcji internetowych będzie wymagała zastosowania silnego uwierzytelniania klienta w przeciwieństwie do aktualnej sytuacji, w której to klient decyduje, czy chce zastosować silne uwierzytelnienie.

Zalecamy jak najszybsze wdrożenie nowej wersji silnej autentykacji EMV.

W jaki sposób Elavon może pomóc?

Firma Elavon jest znana ze swoich możliwości technicznych i skutecznych praktyk biznesowych. Nasza działalność ma szeroki zasięg geograficzny i wyróżnia się wysokiej jakości usługami w zakresie integracji systemów oraz uzyskiwania zgodności regulacyjnej. Wraz z wydawcami oraz organizacjami płatniczymi prowadzimy ciągłe prace ukierunkowane na uzyskanie zgodności z dyrektywą PSD2.

Dyrektywa PSD2 stanowi dla Elavon możliwość zaprezentowania swoim klientom innowacyjnych oraz ciekawych rozwiązań płatniczych i usług doradczych.

W okresie przejściowym oferujemy Państwu wsparcie, zapewniając światowej kasy rozwiązania i porady.

Skontaktuj się z dostawcą usług bramki płatniczej

w celu wdrożenia najnowszej wersji silnej autentykacji EMV.



Więcej informacji uzyskają Państwo,
kontaktując się z zespołem obsługi klienta.

My tworzymy możliwości. Państwo z nich korzystają.

 22 306 03 16

 elavon.pl



Elavon Financial Services Designated Activity Company (Spółka z Ograniczoną Odpowiedzialnością o Wyznaczonym Przedmiocie Działalności). Oddział w Polsce z siedzibą w Warszawie, ul. Puławska 17, 02-515 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 287836, numer REGON 300649197, NIP 2090000825, kapitał zakładowy. Elavon Financial Services Designated Activity Company 6.400.001,00 euro. Elavon Financial Services DAC prowadzi działalność gospodarczą pod nazwą Elavon Merchant Services i podlega nadzorowi Centralnego Banku Irlandii.

Y3604V10120