PolCard
from fiserv.

Przewodnik

PSD2 – silne uwierzytelnienie klienta

Obsługujesz transakcje bezgotówkowe?
Sprawdź, jak działają bezpieczne
płatności cyfrowe.

the speed of life®

Czym jest dyrektywa PSD2 i co oznacza dla Państwa firmy?

Przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. (dalej: PSD2) oraz Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego tę Dyrektywę w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (dalej: RTS), zostały wprowadzone do polskiego prawa w wyniku nowelizacji Ustawy o usługach płatniczych. Przyjęcie dyrektywy zostało wymuszone przez digitalizację, czyli wzrost znaczenia e-commerce i usług świadczonych drogą elektroniczną oraz pojawienie się nowych, dotychczas nieuregulowanych usług płatniczych.

W związku z tym Fiserv wprowadził modyfikacje w aplikacji płatniczej terminala oraz w usługach e-commerce, mające na celu zwiększenie bezpieczeństwa transakcji.

Na czym polega silne uwierzytelnienie klienta (SCA – Strong Customer Authentication)?

Wprowadzenie regulacji PSD2, w szczególności silnego uwierzytelnienia klienta, wpłynęło na zwiększenie bezpieczeństwa obrotu kartowego dla wszystkich podmiotów biorących udział w transakcjach płatniczych. Silne uwierzytelnienie klienta powinno odbywać się w oparciu o zastosowanie co najmniej dwóch z trzech elementów należących do różnych kategorii:

- **wiedza o czymś, co wie wyłącznie użytkownik** (np. kod PIN lub hasło)
- **posiadanie czegoś, co posiada wyłącznie użytkownik** (np. karta płatnicza lub telefon komórkowy)
- **cechy charakterystyczne użytkownika** (np. odcisk palca, rozpoznawanie twarzy lub głosu klienta)

Oferowane przez Fiserv rozwiązania płatnicze umożliwiają przeprowadzanie płatności zgodnie z wymaganiami regulacyjnymi przy jednoczesnym zachowaniu intuicyjnego i szybkiego interfejsu użytkownika.

Główna zmiana na terminalach PolCard polega na tym, że w przypadku wybranych transakcji zbliżeniowych terminal wymaga od posiadacza karty podania kodu PIN (dotychczas transakcje zbliżeniowe poniżej kwoty 100 zł odbywały się bez użycia kodu PIN) lub o zrealizowanie transakcji w sposób stykowy, tj. poprzez włożenie karty do czytnika.

To, kiedy terminal zapyta o PIN, zależy od banku wydającego kartę płatniczą. Może odbyć się to w poniższych sytuacjach:

- gdy łączna kwota poprzednich transakcji bez silnego uwierzytelnienia klienta przekracza 150 euro,
- gdy liczba transakcji bez silnego uwierzytelnienia przekracza 5

Jeżeli korzystają Państwo z terminali lub urządzeń bezobsługowych, które nie są Państwu wypożyczone przez Fiserv – w celu zachowania zgodności należy skontaktować się z dostawcą tych urządzeń, aby dostosować je do wymagań regulacyjnych.

Jakich transakcji nie dotyczy silne uwierzytelnienie klienta?

Nie jest ono wymagane w przypadku następujących typów transakcji:

- **Mail Order/Telephone Order (MOTO) –** prowadzenie sprzedaży typu Mail Order/Telephone Order (MOTO) nie uległo zmianie. Usługi te nie są objęte nowymi regulacjami – wymogiem silnego uwierzytelnienia klienta. Terminale oraz systemy Fiserv dbają o odpowiednie oznakowanie transakcji jako MOTO, dzięki czemu banki autoryzujące transakcje są informowane, że nie należy żądać kodu PIN, ani odmawiać autoryzowania transakcji z powodu braku kodu PIN.
- **inicjowanych przez odbiorcę** (tzw. MIT – Merchant Initiated Transaction) np. płatności cykliczne, opłaty za dodatkowe usługi w hotelu, transakcje przeprowadzone za pomocą anonimowych instrumentów płatniczych np. kart podarunkowych, transakcje wykonywane instrumentami płatniczymi wydanymi poza Europejskim Obszarem Gospodarczym.

3D Secure – technologia, która umożliwia spełnienie wymagania silnego uwierzytelnienia klienta

Jest to międzynarodowa specyfikacja bezpieczeństwa dla płatności kartą w środowisku internetowym, opracowana przez EMVCo. Jest to organizacja powołana przez Visa®, Mastercard®, American Express®, Diners Club International®, Discover Global Network®, JCB®, UnionPay®.

3D Secure jest technologią pozwalająca na uwierzytelnienie transakcji płatniczej, wprowadzoną w celu ograniczenia oszustw internetowych oraz umożliwienia posiadaczowi karty dokonywanie bezpiecznych płatności internetowych.

3D Secure 1.0 vs. 2.0

Zmiana technologii 3D Secure 1.0 na płatności z wykorzystaniem technologii 3D Secure 2.0 zapewnia większe bezpieczeństwo transakcji internetowych. Niektóre banki mogą wciąż obsługiwać wyłącznie płatności 3D Secure 1.0, dlatego Fiserv zamierza wspierać obie wymienione wersje.

Czym jest 3D Secure 2.0?

Jest to zaktualizowana wersja 3D Secure 1.0, która już od pewnego czasu funkcjonuje na rynku w ramach produktów markowych, takich jak Verified by Visa®, Mastercard SecureCode® oraz SafeKey od American Express SafeKey®.

3D Secure 2.0 została stworzona, by zapewnić lepszą szybkość i bezpieczeństwo transakcji. Technologia analizuje między innymi lokalizację dostawy, kwotę zakupów oraz pozwala na uwierzytelnianie transakcji nowymi metodami, na przykład przez odcisk palca czy rozpoznawanie twarzy. 3D Secure 2.0 stanowi podstawową metodę uwierzytelniania wykorzystywaną do spełniania wymogów SCA w zakresie transakcji e-commerce.

Technologia 3D Secure 2.0 może wymagać większej ilości danych w celu potwierdzenia tożsamości posiadacza karty w porównaniu z jego poprzednią wersją.

Weryfikacja dodatkowych informacji pozwala ograniczyć liczbę dokonywanych oszustw na rynku e-commerce.

Czy wspieramy proces 3D Secure?

Fiserv wspiera technologię 3D Secure 1.0 i 2.0 w ramach platformy e-commerce Fiserv.

Akceptanci obsługujący platformę internetową Fiserv uzyskają dostęp do naszego rozwiązania 3D Secure 2.0 automatycznie. Jeżeli nie korzystają Państwo z platformy internetowej zalecamy, aby jak najszybciej skontaktowali się Państwo ze swoim dostawcą bramki płatniczej w celu odpowiedniego przygotowania zmian w mechanizmach płatności.

SCA a płatności elektroniczne bez użycia karty

Płatności elektroniczne bez użycia karty, w większości przypadków muszą spełnić wymogi SCA.

Polecenia przelewu, znane również jako przelewy bankowe w czasie rzeczywistym, oferowane przez banki i systemy takie jak BLIK, wymagają, aby płatnicy płacili za pośrednictwem swojego rachunku bankowego poprzez własny dostęp do bankowości internetowej. Te polecenia przelewu zostały już dostosowane do wymogu SCA. Rozwiązania takie jak PayByLink również spełniają wymogi w zakresie SCA. Przelewy pomiędzy rachunkami własnymi użytkownika w tej samej instytucji nie są objęte wymogiem SCA.

Pomoc

W celu uzyskania pomocy, skontaktuj się z naszym
Centrum Obsługi Klienta. Jest ono czynne 24 godziny na dobę.

(22) 515 30 05

polcard@polcard.pl

www.polcard.pl

Fiserv Polska S.A.
Al. Jerozolimskie 100
00-807 Warszawa
polcard.pl

Sąd Rejonowy dla m. st. Warszawy, KRS 0000061293, NIP: 526-02-10-429,
kapitał zakładowy: 123.609.300 zł, kapitał wpłacony: 123.609.300 zł

fiserv.