Rozwiązania Webowe

Płatności internetowe

Dr inż. Arkadiusz Rzucidło, prof. PRz

Fundamenty płatności online
Czym są płatności internetowe

- transakcje online
- brak fizycznej gotówki
- systemy elektroniczne
- pośrednicy płatności
- integracja z aplikacją webową

Fundamenty płatności online
Czym są płatności internetowe

- Płatności internetowe to przekazywanie pieniędzy bez fizycznego kontaktu.
  - klik → płatność → potwierdzenie
- Za tym stoi cały system:
  - aplikacja webowa
  - system płatności
  - bank
- To jeden z najlepszych przykładów integracji wszystkiego, co poznaliście dotąd.

Fundamenty płatności online
Czym są płatności internetowe

Dlaczego płatności internetowe wymagają integracji wielu systemów?

A. Bo są wolne i integracja to przyśpiesza
B. Bo działają offline
C. Bo obejmują aplikację, operatora płatności i bank
D. Bo nie mają bazy danych i tego nie wymagają

Uczestnicy transakcji

- użytkownik (klient)
- sklep (merchant)
- operator płatności
- bank użytkownika
- bank odbiorcy

Uczestnicy transakcji

- Jedna płatność to nie 2 strony - to cały ekosystem.
  - klient → sklep → operator → bank
- Każdy element musi działać poprawnie.
- Każdy musi uczestniczyć w ekosystemie płatności
- Każdy z systemów musi uczestniczyć w integracji.

Uczestnicy transakcji

Który element pośredniczy między sklepem a bankiem?

A. DNS, współpracując z przeglądarką
B. Operator płatności
C. Router, odpowiednio adresując pakiety
D. Frontend

Typy płatności

- karta płatnicza
- przelew online
- BLIK
- portfele cyfrowe
- płatności mobilne

Typy płatności

- Użytkownik widzi wybór, ale backend musi obsłużyć różne mechanizmy.
  - każdy typ płatności = inny proces
  - Każda z form płatności ma inny scenariusz choć efekt jest ten sam
  - Podobne zabezpieczenia choć inne transakcje

Typy płatności

Który system pozwala na płatność bez wpisywania numeru karty?

A. DHCP
B. BLIK
C. HTTP
D. FTP

Jak działa płatność kartą

- dane karty
- autoryzacja
- komunikacja z bankiem
- decyzja (akceptacja/odrzucenie)
- potwierdzenie

Jak działa płatność kartą

- Proces:
  - wpisujesz dane
  - system sprawdza w banku
  - bank decyduje
- To trwa sekundy, ale to bardzo złożony proces.

Jak działa płatność kartą

- **Karta płatnicza**: To nośnik danych, który umożliwia płatnoś ci bezgotówkowe w sklepach stacjonarnych i internetowy ch.
- Karty dzielą się na karty debetowe i kredytowe, które różni ą się pod względem funkcjonalności.
- **Płatności zbliżeniowe**: Wystarczy włożyć kartę do terminal a płatniczego, a w przypadku większych kwot wymagana jest autoryzacja PIN-em.

Jak działa płatność kartą

- **Płatności przez internet**: Wystarczy **podać dane karty** i zat wierdzić transakcję, często za pomocą SMS lub hasła jedn orazowego.
- **Bezpieczeństwo**: Warto pamiętać o zasadach bezpiecze ństwa, takich jak **nie udostępnianie kodu PIN** innym osobo m oraz **korzystanie z legalnych sklepów** i zabezpieczeń.
- Płatności kartą są **dostępne w większości miejsc**, które ak ceptują płatności bezgotówkowe, co czyni je praktyczny m rozwiązaniem dla codziennych transakcji.

Typy płatności

Kto podejmuje decyzję o akceptacji płatności kartą?

A. Bank użytkownika
B. Sklep
C. Operator
D. Bramka płatnicza

Bramka płatności (payment gateway)

- pośrednik
- przekierowanie użytkownika
- obsługa płatności
- bezpieczeństwo
- integracja z aplikacją

Bramka płatności (payment gateway)

- Bramka płatności to „łącznik”:
  - sklep ↔ system płatności

Przykład:

- Przelewy24 / PayU

Bramka płatności (payment gateway)

- Bramka płatności działa **jako pośrednik między klientem a bankiem**
- Przechwytuje i przetwarzając dane transakcyjne
- Działa podobnie jak czytnik kart w sklepie stacjonarnym
- Łączy się z bankiem w celu przetwarzania płatności doko nywanych osobiście
- Ta sama funkcja w przypadku transakcji internetowych

Bramka płatności (payment gateway)

- Zapewnia łatwość przyjmowania płatności, a klientom poczucie bezpieczeństwa ich danych.
- Proces ten obejmuje:
  - inicjowanie transakcji,
  - szyfrowanie danych,
  - weryfikację przez bank,
  - potwierdzenie sprzedawcy
  - rozliczenie

Bramka płatności (payment gateway)

Dlaczego używamy bramki płatności?

A. Aby przechowywać dane
B. Aby przyspieszyć zakupy
C. Aby zmienić formę płatności
D. Aby bezpiecznie obsłużyć transakcję między systemami

Proces płatności (krok po kroku)

- wybór metody płatności
- przekierowanie do operatora
- podanie danych
- autoryzacja
- powrót do sklepu

Proces płatności (krok po kroku)

- Proces wygląda prosto, ale w tle dzieje się dużo:
  - użytkownik wybiera płatność
  - trafia do operatora (np. PayU)
  - wpisuje dane
  - bank zatwierdza
  - wraca do sklepu
- to wszystko to komunikacja sieciowa + backend + API
-

Proces płatności (krok po kroku)

Który etap odpowiada za decyzję o wykonaniu płatności?

A. Wybór metody
B. Przekierowanie
C. Autoryzacja w banku
D. Powrót do sklepu

Autoryzacja transakcji

- sprawdzenie środków
- weryfikacja użytkownika
- decyzja banku
- zatwierdzenie lub odrzucenie
- bezpieczeństwo

Autoryzacja transakcji

- Autoryzacja to moment kluczowy:
- bank sprawdza:
  - czy masz środki
  - czy to Ty
- wtedy mówi: TAK / NIE

Autoryzacja transakcji

- **Zatwierdzenie**: Autoryzacja polega na potwierdze niu, że osoba dokonująca płatności ma prawo do użycia danej karty lub konta.
- **Rodzaje transakcji:** Obejmuje operacje wykonywa ne zarówno z wykorzystaniem kart płatniczych, jak i przelewy internetowe.
- **Weryfikacja:** Proces ten weryfikuje dane właściciel a karty, stan konta oraz inne istotne informacje, aby zapewnić pomyślne zrealizowanie płatności.

Autoryzacja transakcji

- **Ochrona:** Autoryzacja jest kluczowa dla ochrony p osiadanych zasobów pieniężnych, a w przypadku nieautoryzowanej transakcji należy podjąć odpowi ednie kroki.
- Dzięki autoryzacji transakcji, klienci banków mogą mieć pewność, że ich operacje finansowe są bezpieczne i zgodne z ich uprawnieniami.

Autoryzacja transakcji

Co jest głównym celem autoryzacji?

A. Przyspieszenie płatności
B. Koordynacja zakupów
C. Nic konkretnego to tylko formalność w scenariusz
D. Sprawdzenie poprawności i bezpieczeństwa transakcji

SSL/TLS w płatnościach

- szyfrowanie danych
- ochrona transmisji
- HTTPS
- brak podsłuchu
- podstawa bezpieczeństwa

SSL/TLS w płatnościach

- Płatności bez szyfrowania = katastrofa.
  - dane karty lecą przez Internet
- Dlatego:
  - SSL/TLS = obowiązek

SSL/TLS w płatnościach

- Protokoły te zapewniają:
  - poufność
  - integralność transmisji danych
  - uwierzytelnienie serwera, co jest szczególnie istotne dla transakcji online.
- Certyfikaty SSL/TLS
  - są niezbędne do zachowania zgodności z przepisami,
  - zwiększają zaufanie
  - popraiają SEO, co przekłada się na wzrost zaufania do przedsiębiorstw i ich usług.

SSL/TLS w płatnościach

- Korzystanie z certyfikatów SSL/TLS jest podstawą zapewniającą bezpieczeństwo
  - przechowywania
  - przekazywania danych
  - gwarancją bezpieczeństwa transakcji klientów.

Tokenizacja

- brak przechowywania danych
- karty zamiana danych na token
- bezpieczeństwo
- brak dostępu do danych wrażliwych
- używana przez operatorów

Tokenizacja

- Zamiast numeru karty:
  - system używa „tokenu”
- Czyli:
  - nawet jeśli ktoś przejmie dane → nie wykorzysta ich
  - Token ważny jest na czas transakcji
    - Określony czas
    - Dotyczy jednej transakcji

Tokenizacja

- **Zastąpieniu oryginalnych informacji losowym lub zaszyfrowanym ciągiem znaków**, który nie ma wartości poza autoryzowanym systemem, który go wygenerował.
  - **Słowa lub znaki w tekście** w przetwarzaniu języka naturalnego (NLP), co ułatwia algorytmom analizę danych.
  - **Numer karty płatniczej** w systemach finansowych, chroniąc dane przed kradzieżą i oszustwami.
  - **Prawa do aktywów lub udziały** w projektach w technologii blockchain, umożliwiając cyfrowy obrót aktywami i inwestycje w ułamkowe części nieruchomości, dzieł sztuki czy instrumentów finansowych.

Tokenizacja

- **Płatności cyfrowe -** numer karty jest zastępowany tokenem, który przechowywany
- **Blockchain i cyfrowe aktywa** - tokenizacja pozwala na tworzenie tokenów użytkowych, płatniczych i bezpieczeństwa (security tokens)
- Korzyści:
  - Zwiększone bezpieczeństwo danych
  - Redukcja oszustw

Tokenizacja

Co jest główną zaletą tokenizacji?

A. Ukrywa rzeczywiste dane karty
B. Przyspiesza transmisję
C. Zmienia w czasie formę prowadzenia transakcji
D. Zarządza wysyłką pieniędzy między kontrahentami

3D Secure

- dodatkowe uwierzytelnienie
- SMS / aplikacja bankowa
- potwierdzenie użytkownika
- ochrona przed oszustwem
- standard płatności

3D Secure

- 3D Secure = dodatkowy krok:
  - „czy to na pewno Ty?”
  - SMS / aplikacja bankowa

3D Secure

- Weryfikacja tożsamości użytkownika przed transakcją.
- Jak działa:
  - Użytkownik musi potwierdzić płatność,
    - odpowiedź na pytanie weryfikacyjne
    - podanie jednorazowego kodu SMS, który otrzymuje na swój numer telefonu.
- Usługa chroni przed nieautoryzowanym użyciem środków z karty kredytowej lub debetowej

3D Secure

- Usługa jest automatycznie włączana zazwyczaj przy aktywacji karty, ale można ją włączyć lub wyłączyć przez bankowość internetową lub infolinię banku.
- 3D Secure jest dostępny w wielu bankach

Płatności internetowe – praktyka
Scenariusz: płatność nie przeszła

- brak środków
- odrzucenie przez bank
- błędne dane
- limit transakcji
- problem techniczny

Płatności internetowe – praktyka
Scenariusz: płatność nie przeszła

- Najczęstszy przypadek:
  - użytkownik: „nie działa płatność”
- Możliwe powody:
  - brak pieniędzy
  - błędne dane
  - blokada banku

Płatności internetowe – praktyka
Scenariusz: płatność nie przeszła

Który element decyduje o odrzuceniu płatności?

A. Sklep
B. Bank sklepu
C. Bramka płatnicza
D. Bank użytkownika

Scenariusz: płatność wykonana, brak potwierdzenia

- problem komunikacji
- brak odpowiedzi serwera
- opóźnienie
- problem API
- synchronizacja systemów

Scenariusz: płatność wykonana, brak potwierdzenia

- Płatność przeszła, ale sklep „nie wie”.
  - klasyczny problem integracji systemów
  - zwykle to problem techniczny

Scenariusz: płatność wykonana, brak potwierdzenia

Gdzie najczęściej leży problem w tym scenariuszu?

A. Użytkownik niewłaściwie wpisał dane
B. Źle zaadresowana komunikacja
C. Komunikacja między systemami (API)
D. Bank nie zaakceptował płatności

Scenariusz: fałszywa strona płatności

- phishing
- podobny adres URL
- brak HTTPS
- podszywanie się
- kradzież danych

Scenariusz: fałszywa strona płatności

- Użytkownik myśli, że płaci — ale:
  - dane trafiają do atakującego
  - transakcja wygląda jakby realizowana była poprawnie
  - scenariusz jest łudząco podobny
  - różnica w szczegółach: najczęściej inny odbiorca

Scenariusz: fałszywa strona płatności

Co jest pierwszym sygnałem fałszywej strony?

A. Niepoprawny adres URL lub brak HTTPS
B. Odmienna kolorystyka interfejsu strony
C. Mniejsza szybkość działania serwisu
D. Dłuższe załadowanie strony do przeglądarki

Scenariusz: przejęcie konta

- słabe hasło
- brak 2FA
- phishing
- reuse haseł
- brak świadomości

Scenariusz: przejęcie konta

- Najczęściej:
  - to nie system zawiódł
  - tylko użytkownik
- czynnik ludzki – prawa Murphy'ego
  - Wygoda
  - Pójścia „na łatwiznę"
  - Roztargnienie

Scenariusz: przejęcie konta

Co najbardziej zwiększa ryzyko przejęcia konta?

A. Używanie komunikatorów podczas płatności
B. Używanie tego samego hasła w wielu serwisach
C. Utrzymywanie w przeglądarce kilku aktywnych kart
D. Korzystanie z wielu przeglądarek jednocześnie

Scenariusz: opóźniona płatność

- przeciążenie systemu
- opóźnienie banku
- kolejki transakcji
- sieć
- przetwarzanie

Scenariusz: opóźniona płatność

- Płatność nie zawsze jest natychmiastowa.
  - systemy też mają ograniczenia
  - czasem wynika to ze scenariusza rozliczania
    - Warto zaglądnąć na stronę banku dla pewności – Historia płatności

Scenariusz: opóźniona płatność

Co najczęściej powoduje opóźnienie płatności?

1. Klient przez swoje niezdecydowanie
2. Bramka przez problem z kontaktem ze stroną sklepu
3. Przeciążenie systemów lub banku
4. Odbiorca, nie chce zatwierdzić transakcji

Scenariusz: opóźniona płatność

Co najczęściej powoduje opóźnienie płatności?

1. Klient przez swoje niezdecydowanie
2. Bramka przez problem z kontaktem ze stroną sklepu
3. Przeciążenie systemów lub banku
4. Odbiorca, nie chce zatwierdzić transakcji

Błędy użytkowników

- klikanie w linki
- brak weryfikacji
- słabe hasła
- brak 2FA
- brak świadomości

Błędy użytkowników

- Znowu:
  - największy problem = człowiek
  - czynnik ludzki = najczęstsze błędy

Błędy użytkowników

Który błąd jest najczęstszy przy płatnościach online?

A. Zła przeglądarka internetowa – bez zatwierdzenia
B. Niewłaściwa waluta płatności
C. Zbyt wolny system operacyjny
D. **Brak weryfikacji strony płatności**

Błędy systemowe

- brak obsługi błędów
- brak redundancji
- problemy API
- błędna konfiguracja
- brak monitoringu

Błędy systemowe

- System też może zawieść:
  - brak odpowiedzi
  - błędna integracja
  - kłopoty na poziomie projektowania - deweloper
  - złe/nieintuicyjne scenariusze

Błędy systemowe

Co jest główną przyczyną błędów systemowych?

A. Brak poprawnej konfiguracji i testów systemu
B. Niewłaściwa autoryzacja
C. Zbyt łatwe hasło do systemu płatności
D. Niewłaściwy system operacyjny klienta

Integracja systemów

- sklep ↔ operator
- operator ↔ bank
- API
- komunikacja
- synchronizacja

Integracja systemów

- To najbardziej złożony element:
  - wiele systemów musi działać razem
  - zgranie wyjścia i wejścia każdego z systemów
  - poprawne scenariusze
  - scenariusze błędnego działania (błędnych odpowiedzi)
  - reakcje systemów na „zacięcia”

Integracja systemów

Co jest kluczowe dla poprawnej integracji płatności?

A. Dobranie odpowiedniej waluty transakcji
B. Poprawna komunikacja API między systemami
C. Odpowiednie umiejscowienie w scenariuszu bramki płatności
D. Łatwy interfejs dla użytkownika

Monitoring transakcji

- śledzenie operacji
- wykrywanie błędów
- analiza
- bezpieczeństwo
- raportowanie

Monitoring transakcji

- Bez monitoringu:
  - nie wiesz, co się dzieje
  - trudniej reagować na problemy
  - brak możliwości odtworzenia sytuacji
  - feedback bezpieczeństwa
  - brak źródeł do raportów

Monitoring transakcji

- Bez monitoringu:
  - nie wiesz, co się dzieje
  - trudniej reagować na problemy
  - brak możliwości odtworzenia sytuacji
  - feedback bezpieczeństwa
  - brak źródeł do raportów

Monitoring transakcji

Dlaczego monitoring transakcji jest ważny?

A. Przyspiesza realizację transakcji w Internecie
B. Jest to wymóg ustanowiony prawnie
C. Chroni przeglądarkę klienta
D. Pozwala wykrywać problemy i nadużycia

Ochrona przed oszustwami IDS

- analiza zachowania
- AI
- limity
- weryfikacja
- systemy antyfraudowe

Ochrona przed oszustwami IDS

- Systemy potrafią wykryć:
  - dziwne zachowanie
  - zastosowanie mechanizmów wykrywania
    - Anomalie
    - Sygnatury
  - Historia operacji jako baza uczenia systemów wykrywania
  - Systemy autoryzacji użytkownika (SET)

Ochrona przed oszustwami IDS

Jak system może wykryć próbę oszustwa?

A. DNS
B. Router
C. IDS
D. IP

Rola AI w płatnościach

- analiza danych
- wykrywanie fraudów
- automatyzacja
- szybkie reakcje
- uczenie systemu

Rola AI w płatnościach

- AI:
  - analizuje miliony transakcji
  - monitoring <-> historia operacji
  - sygnatury ataków
  - podejrzane transakcje

Rola AI w płatnościach

Jak AI pomaga w płatnościach?

A. Podpowiada poprawne działanie w transakcjach
B. Sugeruje optymalne scenariusze
C. Wykrywa podejrzane transakcje
D. Ostrzega przed niewłaściwym krokiem

Bezpieczeństwo transakcji

- szyfrowanie
- autoryzacja
- tokenizacja
- monitoring
- kontrola

Bezpieczeństwo transakcji

- Bezpieczeństwo to:
  - wiele warstw
  - mnogość różnych rodzajów zabezpieczeń
  - synergia warstw (F2A)

Bezpieczeństwo transakcji

Który element NIE należy do bezpieczeństwa transakcji?

A. Szyfrowanie połączenia podczas transakcji
B. Tokenizacja danych transakcyjnych
C. Monitoring logów systemów aplikacji webowych
D. Wpisy w DNS jako element ochrony transakcji

Połączenie wiedzy

- web + bezpieczeństwo
- sieci + komunikacja
- bazy + dane
- płatności + systemy
- integracja

Połączenie wiedzy

- Podsumowanie wykładów
  - Bazy danych – przechowują dane (informację)
  - Sieci – zapewniają komunikację
  - Aplikacje webowe – zapewniają funkcjonalność operacyjną
  - wszystko się łączy w globalny system

Połączenie wiedzy

Który element jest wspólny dla wszystkich systemów płatności?

A. Właściwie dobrany i skonfigurowany DNS
B. Funkcjonalna sieć i zespół routerów łączących jednostki
C. Integracja wielu komponentów systemu
D. Wysokowydajne medium komunikacyjne

Dlaczego to ważne

- codzienne użycie
- realne pieniądze
- bezpieczeństwo
- odpowiedzialność
- świadomość

Dlaczego to ważne

- To nie teoria.
  - To codzienne życie
  - Wirtualność
    - Rozszerza funkcjonalność
    - Zapewnia dostęp
    - Ułatwia życie

Dlaczego to ważne

Dlaczego znajomość płatności online jest ważna?

A. Bo dotyczy realnych pieniędzy i bezpieczeństwa użytkownika
B. Bo jest się „na czasie” i obecnie nie stosowanie jej jest „słabe”
C. Bo gotówka to przeżytek
D. Bo nie potrzeba wychodzić z domu żeby zrobić zakupy

Podsumowanie całego bloku

- web
- bezpieczeństwo
- płatności
- integracja
- systemowe myślenie

Podsumowanie całego bloku

- Wiedza z całego bloku powinna umożliwić:
  - rozumieć system
  - rozumieć zagrożenia
  - umieć analizować scenariusze

- to jest poziom „praktyczny IT”

Podsumowanie całego bloku

Co najlepiej świadczy o zrozumieniu całego modułu?

A. Znajomość definicji poszczególnych pojęć
B. Wiedza na temat sieci komputerowych
C. Umiejętność odwzorowania rzeczywistości w bazach danych
D. Umiejętność analizy działania i problemów systemu

KONIEC

- Marshall McLuhan – autorytet w dziedzinie komunikacji
  „We shape our tools, and thereafter our tools shape us.”
  (*„Najpierw kształtujemy narzędzia, a potem one kształtują nas.”*)
- Benjamin Franklin – ojciec założyciel Stanów Zjednoczonych, uczony, filozof
  „An ounce of prevention is worth a pound of cure.”
  (*„Lepiej zapobiegać niż leczyć.”*)
- Tim Berners-Lee – jeden z pionierów WWW
  „The Web does not just connect machines, it connects people.”
  (*„Sieć nie łączy tylko komputerów — łączy ludzi.”*)
- Peter Drucker – specjalista ds. zarządzania
  „The best way to predict the future is to create it.”
  („Najlepszy sposób by przewidzieć przyszłość to ją stoworzyć”)

- ☞ ***Dotyczy to aplikacji, sieci, AI i systemów płatności, które poznaliście.***