Sistemi elektronskog plaćanja

Projektni zadatak master studija

Softversko inženjerstvo i informacione tehnologije - 2025/2026

Agencija za iznajmljivanje vozila

Agencija za iznajmljivanje vozila je *web shop* aplikacija koja omogućava korisnicima da pretražuju i kupuju usluge iznajmljivanja vozila. Aplikacija nudi pregled dostupnih vozila, cena, paketa osiguranja i dodatnih usluga, kao i elektronsku rezervaciju najma.

Kako bi mogli kupovati usluge, korisnici se moraju prvo registrovati a potom prijaviti na *web shop*. Aplikacija omogućava korisnicima:

- kupovinu paketa usluga direktno iz aplikacije, uz mogućnost pregleda detalja svake usluge pre kupovine.
- pregled aktivnih usluga i istorije kupovine (lista prethodno iznajmljenih vozila sa informacijama o ceni i načinu plaćanja)

Sva plaćanja se izvršavaju pomoću *Payment Service Provider*-a (u daljem tekstu PSP), koji predstavlja odvojeni sistem. Korisnici aplikacije, kada odaberu šta žele da kupe, preusmeravaju se na PSP, koji korisnicima nudi različite načine plaćanja.

Plaćanje može da se izvrši na jedan od 4 načina:

1. Plaćanje putem banke
    a. upotrebom platne kartice,
    b. upotrebom QR koda,
2. Plaćanje putem PayPal-a, kroz PayPal nalog,
3. Plaćanje putem kriptovalute

Payment Service Provider (servis koji omogućava plaćanje)

Servis koji omogućava plaćanje (PSP) predstavlja sistem kojim upravlja super admin. Poslovni model PSP-a je posredovanje između različitih servisa za plaćanje i klijenata. Klijenti žele da podrže različite vrste plaćanja, ali ne žele da brinu o bezbednosti datih funkcija i njihovom održavanju, te se odlučuju za upotrebu ovakvog sistema. Klijent u ovom slučaju je Agencija za iznajmljivanje vozila (u daljem tekstu *web shop*), koji se u okviru PSP-a pretplaćuje na proizvoljan skup servisa za plaćanje.

Kada korisnik odabere paket usluga, preusmerava se na PSP, gde bira kojim servisom plaćanja (od ponuđenih servisa na koje se prodavnica prethodno pretplatila) želi da plati odabrani proizvod (Slika 1). Dalja interakcija je definisana u narednim sekcijama za svaki način plaćanja.

U okviru PSP sistema, potrebno je omogućiti:

- dodavanje novih metoda plaćanja,
- uklanjanje postojećih
    - **Napomena: mora biti osigurano da uvek ostane bar jedan aktivan način plaćanja.**
- podršku za različite klijente (ne samo za agenciju)

Svojstva PSP-a:

- **PSP treba da bude *loosely-coupled* sa web shop-om**

PSP treba da ima API koji je prilagođen radu sa raznim sistemima i prodavcima, od sistema koji imaju jednog prodavca (npr. klasična veb-prodavnica) do sistema koji uslužuje više prodavaca.

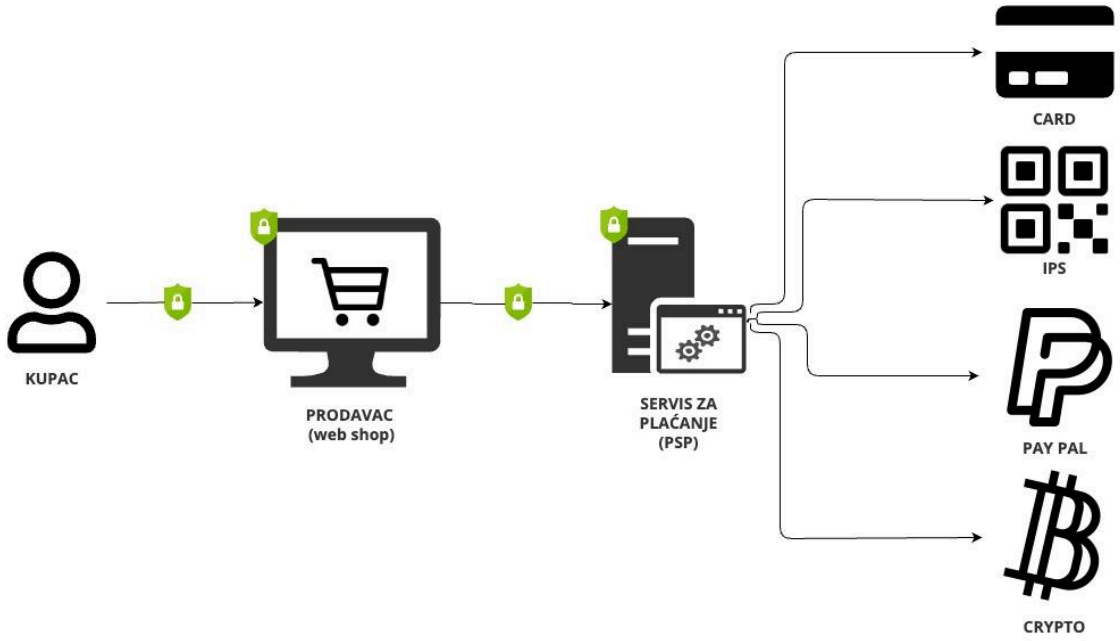
- **PSP treba da bude plagabilan**

  PSP treba da bude plagabilan, svaki vid plaćanja predstavlja jedan plug-in. PSP treba projektovati tako da se novi servisi za plaćanje mogu podržati što jednostavnije (Payoneer, druge kriptovalute, itd).

- **PSP treba da ima arhitekturu koja podržava visoku dostupnost**

  High-availability arhitektura podržava jednostavno skaliranje sistema. Integracija sa novim prodavcem (tipa veb-prodavnica) ili novim načinom plaćanja treba da se omogući bez gašenja PSP-a.

Ceo sistem je neophodno pokrenuti na minimum 2 računara ili na *cloud-u*. Komunikacija HTTPS-om ili nekim drugim *secure* protokolom (poput gRPCs) je obavezna.



Slika 1. Tok komunikacije prilikom plaćanja koji prikazuje PSP kao posrednika u komunikaciji

1. Plaćanje putem banke

Plaćanje putem banke podrazumeva protokol komunikacije između različitih učesnika:

- **Kupac**, korisnik koji izvršava online kupovinu i ima otvoren račun u banci,
- **Prodavac**, vlasnik usluge i ima otvoren račun u banci,
- **Banka prodavca (Acquirer)**, koja pruža servis za online plaćanje, gde kupac unosi podatke o svojoj platnoj kartici,
- **Banka kupca (Issuer)** - proverava stanje računa kupca i odobrava transakciju ukoliko postoje raspoloživa sredstva.

Napomena: Za potrebe ove specifikacije, podrazumevaćemo da računi svih kupaca kao i račun prodavca pripadaju istoj banci - Acquirer banci.

1.1. Plaćanje platnom karticom

Nakon što kupac, u okviru PSP-a, odabere opciju plaćanja putem kartice, tok podataka je sledeći:

1. WebShop formira zahtev za inicijalizaciju transakcije ka PSP-u i šalje podatke prikazane u tabeli 1.

Parametar	**Opis**
MERCHANT_ID	ID prodavca, koji se dobije od PSP-a prilikom pretplate *web shop-a* na plaćanje putem banke
MERCHANT_PASSWORD	Lozinka koja se dobije od PSP-a prilikom odabira plaćanja putem banke. Može da se posmatra i kao api-key koji koristi *webshop* prodavca kako bi svi zahtevi sa tog *webshop*-a bili autentifikovani
AMOUNT	Iznos transakcije
CURRENCY	valuta u kojoj se plaća iznos (plaćanje vršite uvek u istoj valuti ali je potrebno da omogućite podršku za različite valute)
MERCHANT_ORDER_ID	Prodavčev ID transakcije. Generiše se nasumično, od strane web shop-a i služi za identifikaciju i praćenje transakcije
MERCHANT_TIMESTAMP	Prodavčev *timestamp* transakcije
SUCCESS_URL	URL na koji će se kupac preusmeriti ako je transakcija uspešna.
FAILED_URL	URL ne koji će se kupac preusmeriti ako je transakcija neuspešna
ERROR_URL	URL na koji će se kupac usmeriti ako se desila bilo kakva greška.

TABELA 1. PODACI KOJI SE ŠALJU PRILIKOM INICIJALIZACIJE TRANSAKCIJE KA PSP-U

Od navedenih podataka, deo klijent šalje PSP-u sa svakim zahtevom za kupovinu, dok deo treba PSP da poseduje za svakog klijenta. Proceniti optimalnu razmenu podataka.

SUCCESS_URL, FAILED_URL, ERROR_URL predstavljaju unapred dogovoren API na koji PSP može da javi *web shop-u* koji je status transakcije. Na osnovu statusa, korisnik *web shop-a* koji je obavio plaćanje će dobiti prikaz sa odgovarajućom porukom. Ova 3 URL-a ne moraju da se šalju uz svaki zahtev već mogu da se definišu dinamički između *web shop-a* i PSP-a.

2. PSP formira zahtev za dobijanje PAYMENT_URL i PAYMENT_ID parametara koji prosleđuje servisu banke prodavca. Podaci koji se prosleđuju su navedeni u tabeli 2.

Parametar	Opis
MERCHANT_ID	ID prodavca, koji PSP dobije od ACQUIRER banke prilikom inicijalizacije sistema (ovo može biti unapred definisana vrednost između banke i PSPa i ne treba da bude ista kao MERCHANT_ID iz tabele 1)
AMOUNT	Iznos transakcije
CURRENCY	valuta u kojoj se plaća iznos (plaćanje vršite uvek u istoj valuti ali je potrebno da omogućite podršku za različite valute)
STAN (System Trace Audit Number)	ID za praćenje transakcije između PSP-a i banke, generisan od strane PSP-a. Kombinacija parametara MERHCANT_ID + STAN + PSP_TIMESTAMP može da se koristi kako bi se ispratio status transakcije u slučaju da PSP ne primi odgovor od banke.
PSP_TIMESTAMP	*timestamp* transakcije kod PSP-a

Tabela 2. Podaci koji se šalju banci u zahtevu za dobijanje Payment_URL i Payment_ID

3. Banka prodavca proverava da li je dobijen zahtev ispravan i ako jeste generiše PAYMENT_URL i PAYMENT_ID, koji preusmerava kupca sa sajta PSP-a na sajt banke prodavca.
    a. Ispravan zahtev podrazumeva validaciju PSP-a (npr. autentikacija pomoću sertifikata ili HMAC ključeva) kao i validaciju MERCHANT_ID parametra.
4. Na stranici banke prodavca, kupac unosi PAN, SECURITY_CODE, CARD_HOLDER_NAME i datum do kada kartica važi. Izvršava se provera podataka.
    a. Na formi za plaćanje moraju da se nađu logo-i kartica koje sistem prihvata. Svaki broj kartice (PAN) mora biti validiran Lunovom formulom. Datum mora biti u formatu MM/YY uz obaveznu validaciju. Jedna forma (payment url) je vezana za tačno jednu transakciju i potrebno ju je vremenski ograničiti i ograničiti je na samo jedan pokušaj plaćanja.
    b. Iznos za plaćanje na formi nije moguće izmeniti.
5. Banka prihvata zahtev i, ako je ispravan kupac (na osnovu validacije PAN-a, datuma i kontrolnog broja kartice) i ima dovoljno novca, banka rezerviše sredstva. Odgovor, pored statusa transakcije, treba da sadrži i GLOBAL_TRANSACTION_ID ACQUIRER_TIMESTAMP. .
6. Banka prodavca prosleđuje podatke o stanju transakcije, uz STAN, GLOBAL_TRANSACTION_ID i ACQUIRER_TIMESTAMP PSP-u. PSP čuva status i koristi API web shop-a kako bi se kupac prebacio na stranicu koja prikazuje status izvršavanja transakcije (uspeh, neuspeh, greška). U slučaju uspeha, dobija pristup uslugama koje je kupio. GLOBAL_TRANSACTION_ID je dozvoljeno čuvati na *web shop-u* ukoliko ima potrebe.

1.2. Plaćanje QR kodom

Tok podataka kod plaćanja QR kodom i kod plaćanja karticom se razlikuju samo u načinu realizacije stavke 4. Kada se plaća platnom karticom prikazuje se odgovarajuća forma, kada se plaća QR kodom prikazuje se QR kod koji je potrebno skenirati. Za skeniranje koristiti frejm na veb aplikaciji i isključivo raditi skeniranje, a ne kopiranje sadržaja. Ukoliko želite da radite mobilnu aplikaciju, skeniranje raditi preko telefona. QR kod treba da sadrži valutu i iznos koji se plaća, broj računa primaoca (prodavca), naziv primaoca itd. Potrebno je implementirati generator QR koda i validator po uzoru na IPS NBS. Validan QR kod je onaj kod koji omogućava IPS skeniraj & plati iz bilo koje mBanking aplikacije.

2. Plaćanje putem PayPal-a

Kupac koji je odabrao plaćanje putem PayPal-a biva preusmeren na PayPal sajt. Ovde se kupac prijavljuje na svoj PayPal nalog, sa kog izvršava uplatu na nalog prodavca. Radi uspostavljanja ove komunikacije, potrebno je analizirati i upotrebiti PayPal API. Informacije o PayPal transakciji treba čuvati na PSPu i web shop-u slično kao kod kartičnog plaćanja.

3. Plaćanje kriptovalutom

Koristeći Bitcoin API (ili neki alternativni API) izvršiti plaćanje na posebnu Bitcoin adresu koja odgovara *web shop-u*. Iznos za plaćanje u kripto valuti treba da odgovara iznosu u fiat valuti iz *web shop-a* u realnom vremenu. Testiranje plaćanja može se izvršiti postojećim novčanikom (walletom) ili možete implementirati novi novčanik. Za implementaciju koristiti odgovarajuću test mrežu.

BEZBEDNOST

S obzirom na kontektst PSP-a i elektronskog plaćanja, potreban je najviši nivo bezbednosti. Neophodno je proučiti PCI DSS standard, izdvojiti relevantne zahteve i implementirati kontrole koje ispunjavaju date zahteve.

Za PCI DSS standard, potrebno je fokusirati se na:

- *Protect account data* (kompletan zahtev 2)
- *Implement strong access control measures* (kompletan zahtev 4)
- *Track and monitor all access to network resources and cardholder data* (zahtev 5.1)

Napomene

Za svaki od načina plaćanja, potrebno je implementirati i objasniti rešenje u sledećim slučajevima:

- promena iznosa tokom procesa plaćanja
- mehanizam provere statusa transakcije u slučaju da jedan ili više servisa nisu dostupni tokom procesa plaćanja
- mehanizam obrade transakcije u slučaju da korisnik greškom odustane od plaćanja (slučajno zatvori tab, izgubi internet konekciju i sl.)

- dvostruko plaćanje (npr. korisnik dvaput klikne na dugme za plaćanje)

Podela posla je na studentima, studenti se ocenjuju na osnovu njihovog rada i količine posla koje su odradili sa svojim nalogom.

Kontrolne tačke

Timovi	KT 1 25 bodova	Konačna odbrana
Tročlani	● Dizajn sistema. ● Sekvencijalni dijagram toka plaćanja ● Pretplata web shop-a na različite načine plaćanja kod PSP-a. ● Plaćanje karticom. ● Plaćanje putem QR koda.	● Implementacija preostalih načina plaćanja ○ paypal ○ crypto ● Primena PCI DSS standarda ● Visoka dostupnost i skaliranje PSP sistema
Jednočlani	● Plaćanje karticom. ● Sekvencijalni dijagram toka plaćanja	● Plaćanje putem QR koda. ● Primena PCI DSS standarda koji se odnose na kartično plaćanje.

Timovi koji ne izađu na KT1, mogu da nadoknade izgubljene bodove po formuli
bodovi = osvojeni_brodovi_za_funkcionalnosti_sa_KT * 0.8.