PANEVROPSKI UNIVERZITET APEIRON

FAKULTET INFORMACIONIH TEHNOLOGIJA

BANJA LUKA

SRĐAN PERIĆ

ADMINISTRACIJA I PODRŠKA SISTEMA ZA DIGITALNO PLAĆANJE

DIPLOMSKI RAD

BANJA LUKA, NOVEMBAR 2024

PANEVROPSKI UNIVERZITET APEIRON
FAKULTET INFORMACIONIH TEHNOLOGIJA

INŽENJERING INFORMACIONIH TEHNOLOGIJA

ADMINISTRACIJA I PODRŠKA SISTEMA ZA DIGITALNO PLAĆANJE

(DIPLOMSKI RAD)

Mentor
Doc. dr Dražen Marinković

Student
SRĐAN PERIĆ
Index br. /RITP-S

Banja Luka, Februar 2024.

SADRŽAJ

UVOD

Sistemi za plaćanje predstavljaju ključnu komponentu savremenih ekonomija, jer omogućavaju sigurnu, brzu i efikasnu razmjenu novca u različitim poslovnim transakcijama. Razvoj ovih sistema tokom posljednjih nekoliko decenija značajno je unaprijedio način na koji pojedinci i organizacije obavljaju financijske operacije, omogućujući uvođenje novih tehnologija koje poboljšavaju sigurnost, korisnički doživljaj i operativnu efikasnost.

U savremenom društvu, u kojem e-trgovina, mobilni novčanici i bezkontaktni načini plaćanja postaju sve popularniji, sigurnost sistema za plaćanje postaje ključni faktor u očuvanju povjerenja korisnika. U okviru ovog diplomskog rada biće analizirane osnovne komponente sistema za plaćanje, sa posebnim akcentom na tehnologije koje omogućavaju sigurnost transakcija, kao što su P2PE enkripcija, tokenizacija i standardi poput PCI DSS. Također, biće obrađene i administrativne i podrške funkcije koje omogućavaju nesmetano funkcionisanje ovih sistema.

1. Razvoj i značaj sistema za plaćanje u savremenom društvu

1.1. Istorijska evolucija sistema za plaćanje

„Plaćanje podrazumijeva prenos vrijednosti sa jednog agenta na drugi. Kada dva agenta razmjenjuju dobra ili usluge direktno, ovaj prenos se ostvaruje putem trampe. Međutim, postoje značajni problemi povezani trampskom razmjenom. Prema Mangerovoj teoriji o porijeklu novca, vrijednost novca potiče iz njegove sposobnosti da smanji prepreke koje stvara 'dvostruka podudarnost želja', koja ometaju trampu" [1].

„Mengerova teorija se oslanja na Jevonsovu ideju da je za obavljanje razmjene u trampskoj ekonomiji potrebno da jedan potrošač pronađe nekoga ko ne samo da posjeduje željeno dobro već i želi dobro koje taj potrošač nudi zauzvrat. U praksi, rijetko se dešava da dva agenta žele dobra koja posjeduje onaj drugi, još rijeđe da imaju tačne količine tih dobara kako bi se dogovorili o uslovima razmjene, a još rijeđe da se sve to desi u tačnom trenutku kada obe strane žele ta dobra" [1].

„Iako je novac dugo bio sredstvo plaćanja, dokumentirani dokazi sugerišu da su plaćanja između agenata u ekonomiji većinom bila ograničena na jednostavne bilateralne odnose tj. jedan agenat bi proizveo dobro, a potrošač bi ga platio nekim oblikom novca ili robom. Da bi se ekonomski sistemi plaćanja razvili na sofisticiraniji način, bilo je potrebno da nastanu banke koje bi stvorile uslove za daljnje razvijanje tržišta plaćanja. Savremene banke su se razvijale iz različitih početnih tačaka. Bankari srednjovjekovnog Blistog istoka bavili su se ne samo razmijenom novca i davanjem pozajmnica, već su često koristili i razne metode plaćanja. U Evropi, iako su trgovci i bankari mogli posmatrati ove prakse prilikom trgovine sa teritorijama Bliskog istoka, ne postoji direktan dokaz da su sredstva plaćanja sa Bliskog istoka direktno preuzeta. Umjesto toga, u mjestima gdje je u opticaju bilo mnogo različitih vrsta kovanica, kao što je Venecija u 13. vijeku, mjenjači novca su proširili svoju ulogu vrednovanjem novca nudeći usluge plaćanja i drugih bankarskih usluga zasnovanih na depozitima koje su držali. Slično tome, u Londonu sredinom 17. vijeka, porijeklo bankarstva može se pronaći među zlatarima, koji su razvili sličan bankarski posao zasnovan na specijalizovanoj usluzi pružanja skladišnih uslova za bezbijedno čuvanje imovine" [1].

Slika 1 - „Pregovaranje u zalagaonici", iz Cocharelli Treatise (oko 1330), Britanska biblioteka, MS 27695, fol. 7v.

„Bilo da su zapadnoevropske banke nastavle kao mjenjači novca ili zlatari, trgovci su mogli da depozituju svoje kovanice kod njih u zamijenu za potvrdu. Transakcije su se zatim mogle obavljati ili putem knjiga mijenjača ili zlatara i čak prenosom potvrda koje su izdali. U nekim sistemima, poput onih u kontinentalnoj Evropi, pretežno su se koristili metodi plaćanja zasnovani na računima, gdje su transferi vršeni sa jednog bankarskog računa na drugi“ [1].

„Do početka četrnaestog vijeka, venecijanski zapisi pokazuju da su korisnici računa u istoj banci mogli da obavljaju plaćanja međusobno putem knjižnih prenosa. Međutim, ne postoji konačan dokaz da su ove banke redovno prihvatale međusobne obaveze. Do sredine četrnaestog vijeka, nakon niza lokalnih bankrota, počeli su pozivi u Veneciji na osnivanje javne banke koja bi omogućila obavljanje plaćanja bez kreditnog rizika inherentnog komercijalnim bankarima. Njena razvojna faza trajala je više od dva vijeka, a realizovana je tek kada je 1587. godine osnovana Banco di Rialto“ [1].

Slika 2 - Banco di Rialto u Veneciji

„Vijekovima kasnije, banke su primjetile opadanje uloge gotovine i kao odgovor na to, nekoliko centralnih banaka je javno objavilo interne napore za proučavanje digitalnih valuta centralnih banaka (CBDC) za maloprodajna plaćanja, veleprodajna plaćanja ili oboje. Banke su tradicionalno igrale centralnu ulogu u podršci plaćanja, tako da bi njihovo uklanjanje iz centra ovog sistema moglo preoblikovati bankarstvo i šire, finansijsko tržište“ [1].

„Važno je napraviti razliku između veleprodajnih i maloprodajnih plaćanja. Veleprodajna plaćanja su visokoprioritetni i obično veliki transferi koji se vrše između finansijskih institucija za njihove vlastite račune ili u ime njihovog klijenta i obično se poravnavaju putem specijalizovanim međubankarskih sistema za poravnanje. Maloprodajna plaćanja, s druge strane, predstavljaju transakcije niže vrijednosti između pojedinaca, preduzeća i vlada u oblicima kao što su gotovina, čekovi, bankovni transferi i transakcije debitnim i kreditnim karticama“ [1].

1.2. Pojava e-trgovina i online plaćanja

“Prvi digitalni sistem za elektronsko plaćanje pon nazivom ‘Ecash’, predstavio je David Chaum. Omogućio je korisnicima da obavljaju anonimne online transakcije. Međutim, sistem nije stekao veliku popularnost zbog tehničkih problema i regulatornih prepreka“ [2].

„Ubrzo nakon Ecash-a, 1998. godine, PayPal se pojavio kao alternativa tradicionalnim metodama plaćanja poput čekova i novčanih naloga. Omogućio je korisnicima da šalju i primaju novac putem interneta koristeći adresu elektronske pošte i povezani bankovni računi ili kreditnu karticu. PayPal-ov jednostavan interfejs i lagan proces transakcije pomogli su mu da postane glavna platforma za plaćanje online aukcijama i e-commerce sajtovima“ [2].

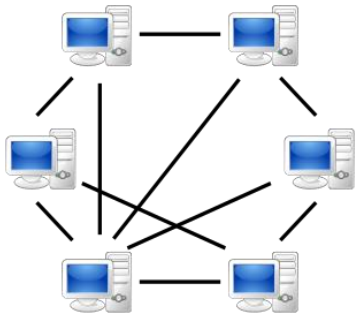
Slika 3 - Grafički interfejs PayPal-a u 1998. godini

„Kako je popularnost online kupovine rasla početkom 2000-ih, online trgovci su tražili načine da učine digitalna plaćanja još pogodnijim za svoje korisnike. Kompanije poput Amazon i Google su uveli vlastite sisteme za plaćanje, poznate kao Amazon payments i Google checkout“ [2].

„U 2011-toj godini, postignut je još jedan značajan korak sa lansiranjem Square-a, servisa za plaćanje koji omogućava malim preduzetnicima da prihvataju plaćanja kreditnim karticama koristeći samo mobilni uređaj i čitač kartica. Ovo je revolucionisalo procesiranje plaćanja za nezavisne poslodavce i male trgovce“ [2].

Slika 4 - POS Terminal i čitač kartica Square kompanije

„Poslijednjih godina, uspon kriptovaluta doveo je do pojave novih metoda digitalnog plaćanja kao što su BitCoin, Ethereum, Doge Coin. Ovi decentralizovani sistemi plaćanja omogućavaju korisnicima da obavljaju peer-to-peer (tzv. P2P) transakcije bez potrebe za posrednicima kao što su banke ili procesori plaćanja“ [2].



Slika 5 - Grafički prikay P2P komunikacije

„Sve u svemu, pojavljivanje digitalnih sistema plaćanja fundamentalno je promijenilo način na koji obavljamo transakcije. Od ranih dana Ecash-a pa do uspona kriptovaluta, digitalna plaćanja su postala sve prisutnija i raznolika, čineći slanje i primanje novca putem interneta lakšim i pogodnijim nego ikada“ [2].

„Savremene transakcije se stalno pomjeraju sa transakcije zasnovanih na gotovini ka onima koji se zasnivaju na elektronskim plaćanjima. Svuda prisutna povezanost ICT-a značajno doprinosi transformaciji finansijskog tržišta i njihovih operacija“ [3].

“Trend ka digitalizaciji i korištenju interneta doveo je do značajnih promijena u načinu na koji globalna ekonomija funkcioniše. Pojava širokog spektra aplikacija finansijske tehnologije (FinTech) omogućava potrošačima da pređu sa konvencionalnog sistema plaćanja zasnovanog na gotovini. Digitalna plaćanja postaju norma u svakodnevnom životu ljudi. Ovi brzi razvoji u finansijskom sektoru dovode do izuma mnogih tehnologija digitalnog plaćanja, kroz koje i osobe koje plaćaju i osobe koje primaju novac, koriste digitalne aplikacije za slanje i prijem novca. Tako, sistem plaćanja brzo prelazi sa novca zasnovanog na kovanicama i papirnom novcu na digitalne oblike plaćanja koji su praktičniji, brži i isplatljiviji“ [4].

1.3. Porast mobilnih novčanika i bezkontaktnih načina plaćanja

„Porast pametnih telefona je stvorio novu eru financijskih transakcija. Kako je sve više ljudi počelo da koristi pametne telefone u različite svrhe, digitalna plaćanja putem mobilnih novčanika postala su sve više popularnija. Mobilni novčanici omogućavaju korisnicima da sigurno čuvaju podatke o svojim debitnim i kreditnim karticama i da ih koriste za različite transakcije“ [2].

„Sa dodatnim pogodnostima mobilnog plaćanja, bezkontaktna plaćanja postala su norma jer su omogućila potrošačima da obavljaju transakcije bez dodirivanja kartice. Bezkontaktna plaćanja omogućavaju korisnicima da tapnu karticu na čitač kako bi izvršili plaćanje. Ova metoda nije samo brža, već je i sigurnija od tradicionalnih kartičnih plaćanja, jer uključuje minimalan kontakt“ [2].

Slika 6 - Bezkontaktno plaćanje u praksi

„Pandemija COVID-19 je posebno ubrzala prihvatanje mobilnih novčanika i bezkontaktnih plaćanja. S obzirom da se virus može prenijeti kontaktom, potrošači se odlučuju za bezkontaktna plaćanja kako bi smanjili kontakt sa drugim osobama“ [2].

„Popularnost mobilnih novčanika i bezkontaktnih plaćanja ne pokazuje znakove usporavanja. Kako sve više preduzeća usvajaju digitalna plaćanja, potrošači će sve više birati ove metode jer nude veću pogodnost, brzinu i sigurnost“ [2].

2. Osnovne komponente sistema za plaćanje

Sistemi za plaćanje se sastoje od tri ključna dijela:

- **Arhitektura sistema** – uključuje POS terminale koji omogućavaju unos podataka o transakcijama, mrežnu infrastrukturu za prenos podataka i servere za čuvanje i obradu tih podataka

- **Funkcionalnosti sistema** – obuhvataju obradu transakcija, što znači verifikaciju i čuvanje načina plaćanja, tokenizaciju koja omogućava bezbijednu zamjenu osjetljivih podataka i intergracije sa drugim sistemima

- **Primjena sistema za plaćanje** – sistemi za plaćanje pronalazi svoju široku primjenu u različitim industrijama, kao što su restorani, maloprodaja i mnogi drugi

2.1. Point-of-Sale (POS) Terminali

“POS terminal kombinuje hardverske i softverske komponente kako bi obezbijedio efikasan proces naplate. Hardver obično uključuje računar ili tablet, skener barkodova ili čitač kartica, fioku za gotovinu i štampač računa. POS softver koji se pokreće na terminalu omogućava preduzetnicima da bilježe i prate prodaju, upravljaju inventarom i da generišu izvještaje u stvarnom vremenu” [5].

“Mnogi POS terminali nude vrijedne funkcionalnosti koje pojednostavljuju poslovne operacije. To može uljučivati na alate za upravljanje odnosima sa kupcima (CRM – engl. Customer Relationship Management), programe lojalnosti, upravljanje zaposlenima, integraciju sa drugim poslovnim softverima kao što su sistemi za računovodstvo ili upravljanje inventarom” [5].

Slika 7 - Point-of-Sale terminal kompanije NCR Corporation

2.1.1. Princip rada Point-of-Sale terminala

“Princip rada POS terminala je veoma jednostavan i može se opisati u šest jednostavnih koraka.

- Unos transakcije – Kada je kupac spreman za kupovinu, unosimo detalje transakcije u POS terminal koje može biti ručno ili skeniranjem bar koda.

- Izračunavanje ukupnog iznosa – POS terminal izračunava ukupni iznos koji treba da se plati na osnovu unesenih podataka o transakciji, uključujući poreze i popuste

- Izbor načina plaćanja – kupac može da odabere način plaćanja kao što su kreditna kartica, debitna kartica ili gotovina

- Prihvatanje plaćanja – Ako kupac odabere kartično plaćanje, POS terminal sigurno obrađuje plaćanje šifrovanjem podataka sa kartice i slanjem autorizacije

- Autorizacija i verifikacija – POS terminali komuniciraju sa procesorom plaćanja ili bankom koja preuzima plaćanje kako bi provjerio podatke sa kartice i dostupna sredstva. Transakcija se odobrava ili odbija na osnovu dobijenog odgovora

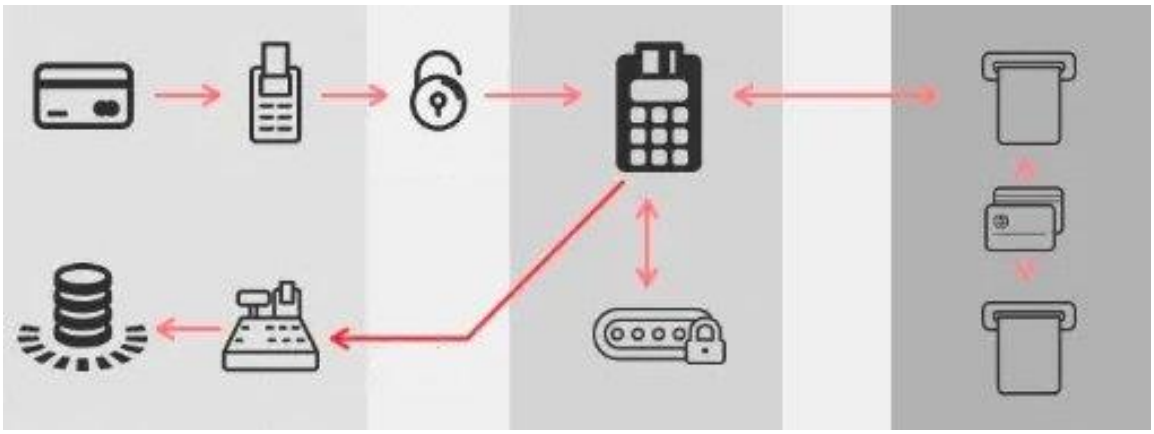
- Završetak transakcije – Ako je plaćanje odobreno, POS terminal prikazuje “transakcija završena” na ekranu, zatim se štampa račun i ažurira u evidenciju o prodaji i novoima inventara” [5]

2.1.2. Važnost POS terminala u poslodavstvu

“POS terminali pojednostavljuju proces naplaćivanja automatskim izračunavanjem i eliminiše manuelne greške. Također, omogućava efikasno skeniranje ili unos informacija o proizvodu, izračunava ukupni iznos koji treba platiti i generiše tačne račune” [5].

“POS terminali također prihvataju različite metode plaćanja, uključujući kreditne kartice, debitne kartice i bezkontaktne metode poput mobilnih novčanika (ApplePay) ili uređaje sa NFC tehnologijom. Nudeći više opcija plaćanja, možete zadovoljiti preferenciranje kupaca i povećati vijerovatnoću zaključenja prodaje“ [5].

„POS terminali prioritizuju sigurnosti šifrovanjem osjetljivih podataka o kupcima nakon plaćanja, poput informacija o karticama. Ovo enkriptovanje pomaže u zaštiti od proboja podataka i neovlaštenog pristupa, čuvajući privatnost kupaca i smanjujući rizik od prevara. Sigurnim sistemom, poslodavac može izgraditi povjerenje kod kupaca i održati pozitivan ugled“ [5].



Slika 8 - Jednostavan prikaz enkripcije na POS terminalu

„POS terminali često uključuju funkcije za upravljanje prodajom i zalihama. Oni prate podatke o prodaji, pružajući uvid u najprodavanijim proizvodima, periodima sa najvećom prodajom i obrazcima kupovine. Ove informacije omogućavaju donošenje informisanih poslovnih odluka, kao što su obnavljanje zaliha i modifikacija cijena. Također, POS terminali automatski ažuriraju količine zaliha nakon svake prodaje, smanjujući šanse za nedostatak ili višak zaliha“ [5].

„Terminali su dizajnirani da podrže rast i širenje poslovanja. Oni mogu veoma lako podnijeti povećane obime transakcija i podržati više kasa ili lokacija. Dodatni POS terminali se mogu bez problema integrisati u sistem kako se poslovanje širi. Ova skalabilnost omogućava poslodavcima da se prilagode promijenljivim potrebama, efikasno upravljaju većim obimom prodaje i održavaju kvalitet usluge tokom rasta“ [5].

„Praćenje prodaje u realnom vremenu pustem POS terminala omogućava praćenje prodaje u svakom trenutku. Ovo omogućava poslodavca da bude informisan o finansijskom stanju svog poslovanja, prateći prodaju na dnevnom ili mjesečnom nivou“ [5].

2.2. Čitači kartica (engl. Card Readers)

“Čitač kartica je uređaj dizajniran za dekodiranje informacija sa magnetne trake ili ugrađenog čipa na kreditnoj ili debitnoj kartici. Ove informacije obično uključuju detalje o vlasniku kartice, broj računa, datum isteka kartice i sigurnosne kodove. Čitači kartica mogu obrađivati ove podatke koristeći magnetne trake, čitače mikročipa ili bezkontaktne NFC tehnologije, u zavisnosti od vrste kartice. Obično se koriste u sistemima za plaćanje poput POS terminala ili bankomata, omogućavajući trgovcima i pružaocima usluga da sigurno obrade transakcije elektronskim putem. Savremeni sistemi su brži i sigurniji u poređenju sa starijim metodama koje su se oslanjale na ručne otiske ili kopiranje podataka sa kartice“ [6] [7].

Slika 9 - Čitači kartica kompanije Equinox Payments u raznim modelima

2.2.1. Tehnologije plaćanja putem čitača kartica (Magnetna traka, EMV čip, NFC)

„**Magnetna traka** je tradicionalna metoda koja koristi magnetnu traku na poleđini kartice, koja skladišti statične podatke poput broja kartice, datuma isteka kartice i servisnog koda. Međutim, tehnologija magnetne trake se smatra manje sigurnom zbog njene ranjivosti na 'skimming’” [8].

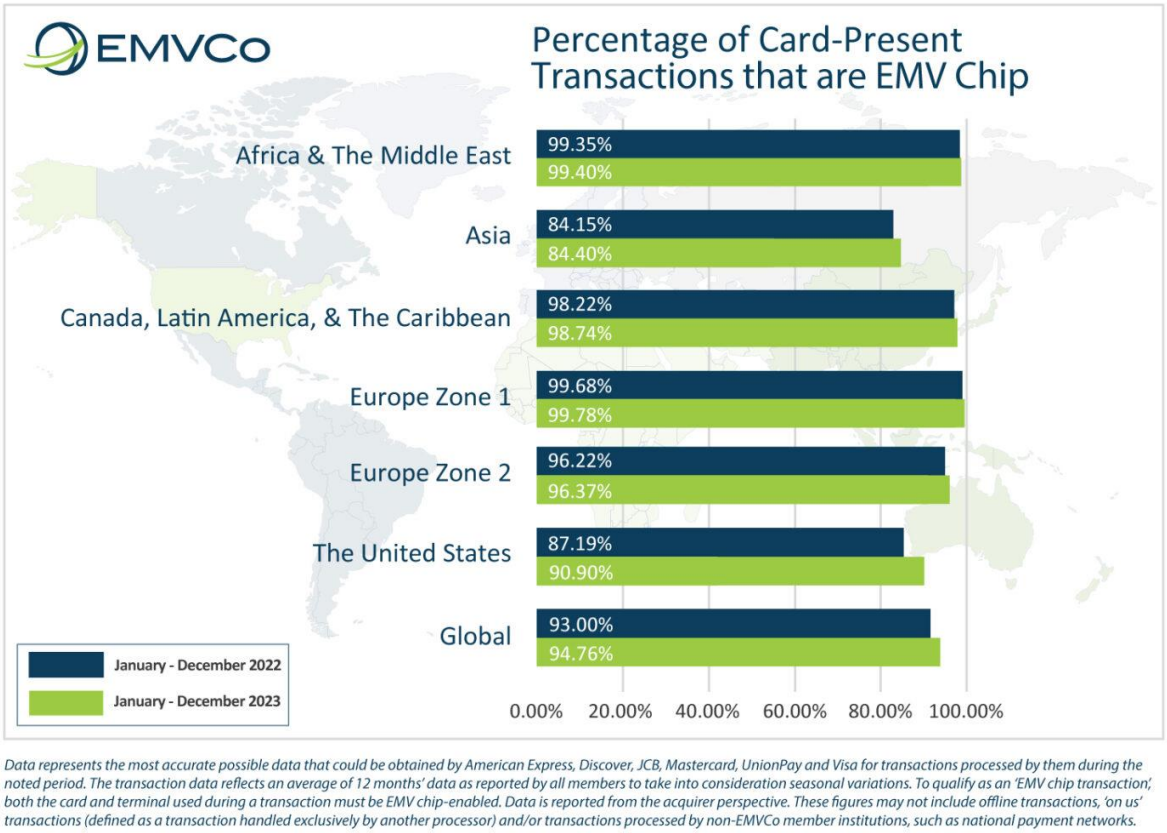
Slika 10 - Magnetna traka na čitaču kartica

„**EMV čip kartice**, ime EMV nastaje od kombinovanja brendova Europay, MasterCard i Visa. Ove kartice sadrže ugrađeni mikročip koji skladišti šifrovane podatke i zahtijeva PIN authorizaciju“ [8].

Slika 11 - Primjer EMV čip kartice

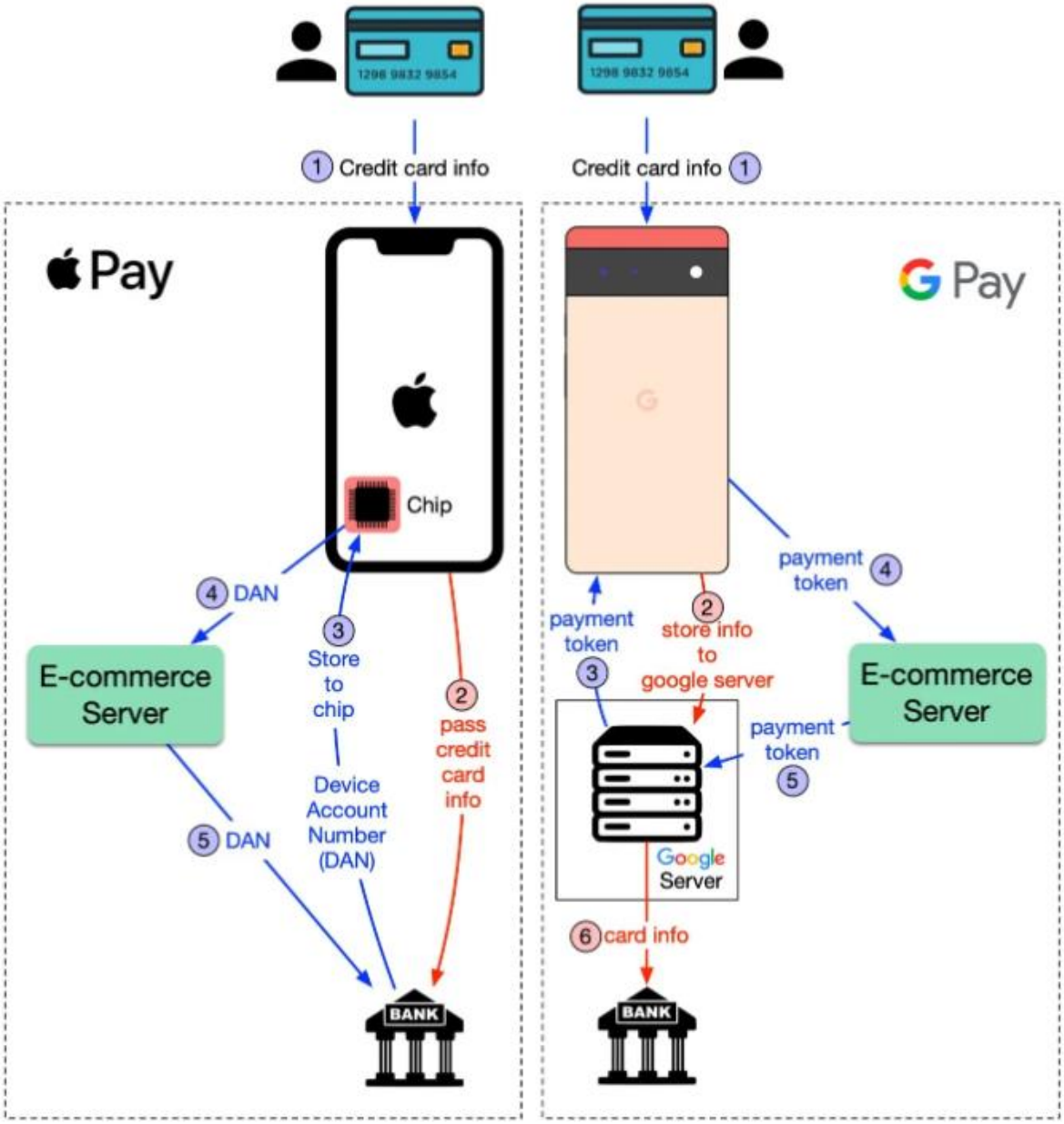
„Tehnologija EMV čipa značajno smanjuje rizike od prevarantskih transakcije“ [8].

„U posljednjem izvještaju za četvrti kvartal (engl. quarter) 2023. godine, globalno je 94,76% transakcija izvršeno putem EMV čip kartica. Ovi podaci predstavljaju najtačnije moguće informacije koje su prikupili American Express, Discover, JCB, MasterCard, Visa, UnionPay i Maestro“ [9].



Slika 12 - Prikazanost korištenja EMV čip kartica u različitim regijama Svijeta

„**Near Field Communication (NFC)** tehnologija omogućava bezkontaktna plaćanja putem mobilnih novčanika kao što su ApplePay i GooglePay. Kada korisnik prinese ili ubliži svoj pametni telefon sa NFC tehnologijom na čitač kartica ili POS terminal, podaci sa kartice se bezbijedno prenose korištenjem radio talasa“ [8].



Slika 13 - Grafički prikaz o tome kako ApplePay i GooglePay raspolažu sa podacima

2.3. Sistemi za obradu plaćanja (End-to-End payment processing)

„Sistemi za obradu plaćanja od početka do kraja omogućavaju online kompanijama da upravljaju svojim procesima plaćanja od početka do kraja na jednom mjestu. Ovi sistemi objedinjavaju sve

informacije koje su uključene u obradu plaćanja, dajući e-commerce platformama potpunu vidljivost tih procesa“ [10].

„Pošto kupci koriste različite metode plaćanja, online trgovci moraju da sarađuju sa pružaocom riješenja koji može obraditi i centralizovati sve ove metode plaćanja na istoj platformi. Sistemi za obradu plaćanja od početka do kraja treba da se automatski skalira, omogućavajući kompanijama da odrađuju velike količine kartica u bilo kojem trenutku“ [10].

„Pružatelji sistema za obradu plaćanja od početka do kraja razlikuju se od onih koji nude samo backend obradu plaćanja. Backend procesor plaćanja pruža trgovcima usluge i infrastrukturu potrebnu za obradu plaćanja kupaca. Online trgovci koji samo trebaju obradu kreditnih kartica mogu se udružiti sa backend procesorima plaćanja. Međutim, za obradu plaćanja od početka do kraja, trgovci bi trebali sarađivati sa pružaocima koji nude end-to-end rješenje“ [10].

„Kompanije koje pružaju usluge plaćanja (PSP) razlikuju se od banaka jer su modernije kompanije, specijalizovane isključivo za prenos novca. Također, fokusirani su na poboljšanje iskustva obrade plaćanja od početka do kraja. Kao takvi, online trgovci će vidjeti mnoge koristi od toga što će prepustiti obradu plaćanja specijalizovanim kompanija koje pružaju ove usluge, umjesto svojoj banci“ [10].

„End-to-end procesuiranje plaćanja uključuje nekoliko koraka i entiteta koji omogućavaju sigurnu i efikasnu obradu transakcija. End-to-end procesovanje funkcionište na slijedeći način:

- **Trgovac** – Online poslovanje koje prihvata plaćanje putem kartica za obavljanje prodaja
- **Akviziter** – Financijska institucija koja upravlja računom trgovca, procesuira plaćanje i premješta sredstva u ime trgovca
- **Vlasnik ili nosilac kartice** – Kupac koji koristi svoju karticu za obavljanje kupovine
- **Izdavač** – Banka koja izdaje kreditne i debitne kartice korisnicima
- **Kartične mreže** (šeme) – Mreže kao što su Visa i MasterCard koje upravljaju procesom transakcijama kreditim i debitnim karticama

Pored ovih glavnih funkcija, postoje i druge veoma važne komponente:

- **Payments Gateway**– Tehnologija koja omogućava online prihvatanje plaćanja, tako što prikuplja podatke o kartici i šalje ih procesoru plaćanja

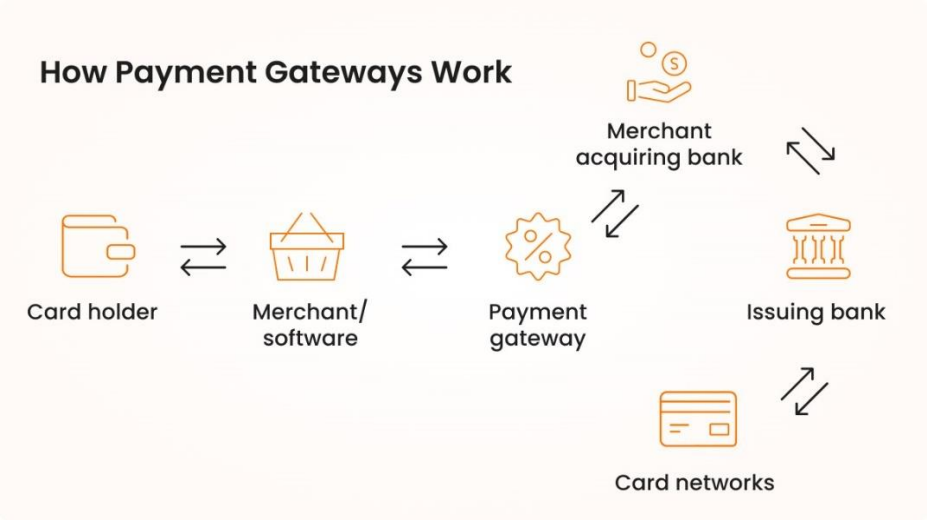
- **Payments Processor** – Servis koji povezuje akvizitersku banku trgovca sa kartičnim mrežama za obradu transakcija“ [10]

2.3.1. Payments Gateway

“Payments Gateway je tehnologija koja djeluje kao posrednik u elektronskim finansijskim transakcijama, obezbijeđujući nesmetano procesuiranje sredstava i sigurno autorizovanje transakcija. Payments Gateway, također omogućuje preduzetnicima da sigurno upravljaju

različitim metodama plaćanja, uključujući digitalne novčanike, debitne kartice i kreditne kartice" [11].

"Povezujući kupce, preduzetnike i finansijske institucije, payments gateway konsoliduje ove interakcije u kohezivnu platformu. Obično, payments gateway naplaćuje naknadu za svaku obrađenu transakciju, čime se obezbjeđuje sigurnost i efikasnost finansijskih razmjena" [11].

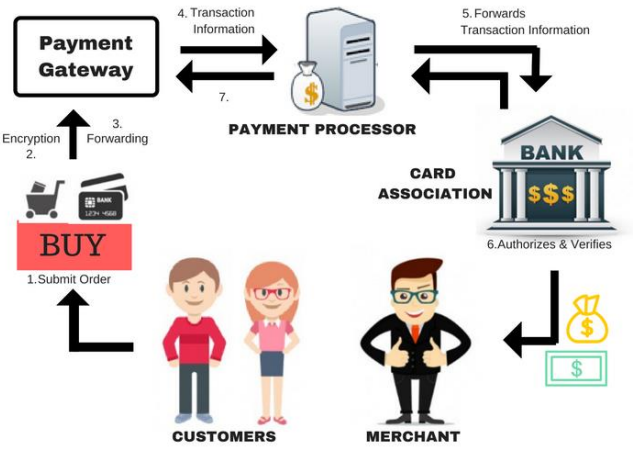


Slika 14 - Grafički prikaz Payments Gateway procesa

"Payments Gateway sistemi su ključni za svaki web sajt koji omogućava online kupovinu putem kreditnih kartica, debitnih kartica ili drugih metoda plaćanja. Osim što omogućavaju nesmetane transakcije, pomožu u prevenciji prevara, smanjuju greške u obradi, ubrzavaju procese transakcija i pojednostavljuju uskljađivanje" [11].

"Neki od osnovnih benefita Payments Gateway-a su:

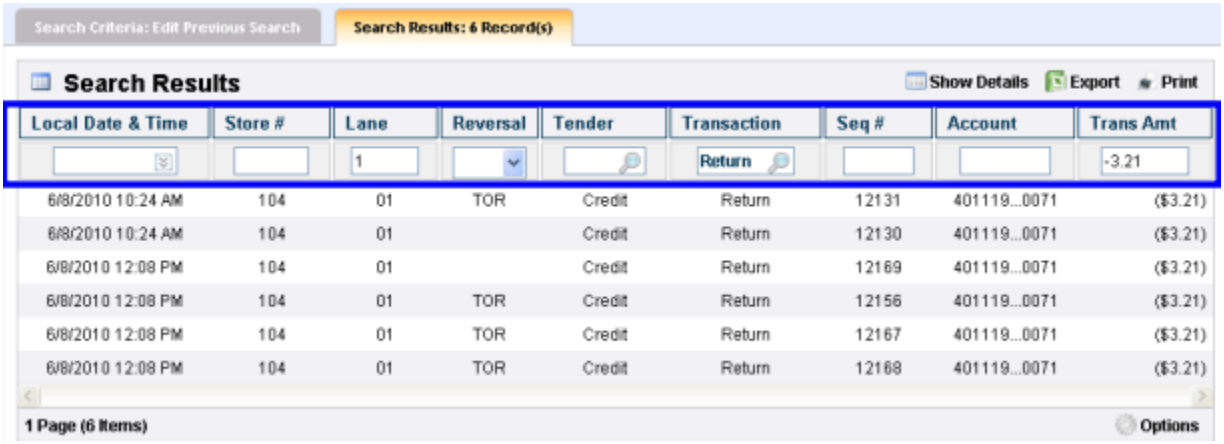
Enkripcija tokom procesovanja transakcije, štiteći korisnika od neovlaštenog pristupa ili krađe dok transakcije putuje od POS terminala, servera preduzeća i finansijskih institucija" [11].



Slika 15 - Ilustrativan prikaz putanje transakcije od korisnika pa sve do banke

„Payments Gateway prenosi enkriptovane podatke o transakciji do banke preduzeća, koja ih dalje prosljeđuje banci korisnika ili odgovarajućem procesoru plaćanja. U ovom segmentu **autorizacije** se vrši provjera detalja transakcije, uključujući stanje na računu i validnost načina plaćanja, prije nego što se odobri ili odbije transakcija i payments gateway odmah prenosi odgovor nazad preduzeću.

Payments Gateway sistemi često nude preduzećima korisne podatke, uključujući istoriju transakcija i upravljanje povraćajem (engl. refund) sredstava, omogućavajući analizu i optimizaciju operacija plaćanja“ [11].



Slika 16 - Primjer kolektovanja i navigacijom podataka u Payments Gateway portalu za preduzetnika

„Korištenjem sofisticiranih bezbjednosnih mjera kao što su algoritmi za detekciju prevara, sistemi za verifikaciju adresa (AVS) i provjere vrijednosti verifikacije kartice (CVV), payments gateway sistemi aktivno detektuju i blokiraju potencijalno opasne transakcije, efikasno smanjujući rizike poslodavcu“ [11].

„Payments Gateway predstavlja ključni element u okviru sistema za elektronsku obradu plaćanja. Kao napredna tehnologija, preuzima odgovornost za prenos informacija o korisniku do banke koja vrši akviziciju trgovca. Nakon toga, banka precesuira transakciju putem svog sistema.

Payments Gateway sistem funkcioniše na sljedeći način:

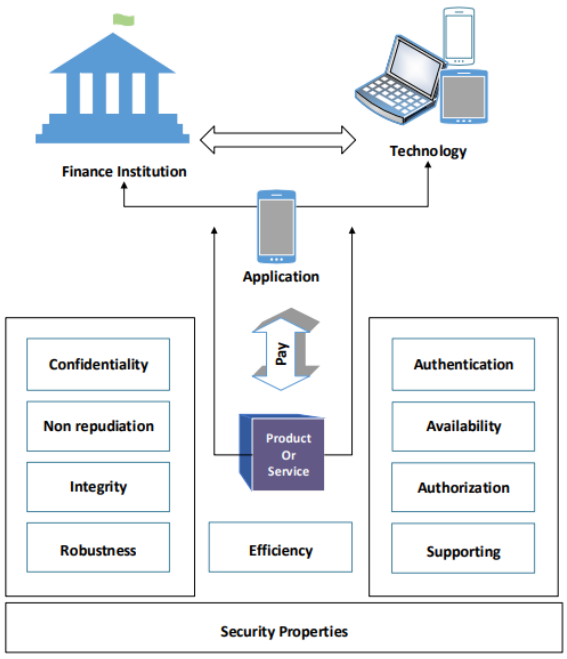
- **Inicijalizacija transakcije** – Korisnik bira proizvode ili usluge na sajtu ili aplikaciji preduzeća i prelazi na naplatu, unoseći podatke o plaćanju, kao što su podaci o kreditnoj kartici ili digitalnom novčaniku
- **Enkripcija podataka** – Dostavljeni podaci o plaćanju enkriptovani su od strane sistema korištenjem SSL ili TSL protokola, čime se obezbjeđuje zaštita od neovlaštenog pristupa tokom prenosa
- **Prenos podataka ka serveru preduzeća** – Enkriptovani podaci o plaćanju šalju se na server preduzeća, gdje se sigurno čuvaju i proslijeđuju sistemu za plaćanje na obradu

- **Prosljeđivanje podataka o transakciji** – Payments Gateway prima enkriptovane podatke o transakciji sa servera preduzeća i prosljeđuje ih procesoru plaćanja i banci koja vrši akviziciju za dalju obradu
- **Verifikacija transakcije** – Banka koja vrši akviziciju šalje podatke o transakciji banci korisnika ili odgovarajućem procesoru plaćanja na autorizaciju, provjeravajući detalje kao što su stanje na računu i validnost načina plaćanja
- **Odobrenje ili odbijanje transakcije** – Na osnovu verifikacije, banka korisnika ili procesor plaćanja odobrava ili odbija transakciju. Odgovor se prosljeđuje serveru preduzeća putem banke koja vrši akviziciju
- **Komunikacija statusa transakcije** – Payments Gateway sistem komunicira status transakcije (odobreda ili odbijena) na POS terminal ili aplikaciju preduzeća, pružajući odgovarajuće poruke korisniku. Odobrene transakcije nastavljaju sa ispunjenjem porudžbine, dok odbijene traže alternativne metode plaćanja“ [11]

3. Bezbjednost sistema za plaćanje

“Zaštita može biti glavni problem kod elektronskih metoda plaćanja jer bez bezbjedne razmjene industrijskih informacija i sigurnih elektronskih monetarnih transakcija putem mreža, niko neće vjerovati da je njihova upotreba bezvrijedna. Korisnici zahtjevaju povjerljivost, autentifikaciju, integritet podataka, kao i neprorječivost kao ključne potrebe za sigurno obavljanje plaćanja putem interneta“ [12] [13].

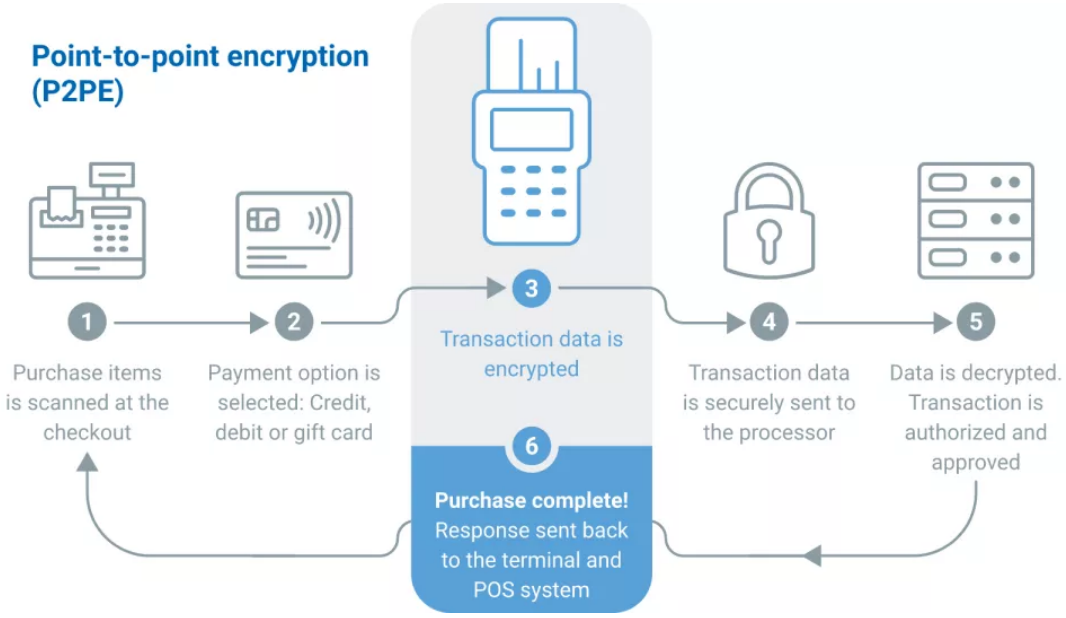
„Elektronski sistemi plaćanja moraju imati sve navedene atribute zaštite, jer korisnici sigurno neće vjerovati sistemu za e-plaćanje koji nije bezbijedan. Uz to, provjerenje je izuzetno važno kako bi se osigurala prihvaćenost od strane klijenta. Ova oblast će pružiti najviše sigurnosne karakteristike kako bi se spriječila prevara u elektronskim plaćanjima, uz pregled elektronskih transakcije i primjenjenim sigurnosnim mjerama“ [14].



Slika 17 - Bezbjednosni atributi elektronskih plaćanja

3.1. P2PE (Point-to-point) Enkripcija

“Point-to-point enkripcija (P2PE) je tehnološki standard za pretvaranje osjetljivih podataka u nečitljiv oblik radi njihove zaštite. Enkriptovani podaci ne mogu se čitati niti mjenjati od strane bilo koga ko nema odgovarajući ključ za dekripciju kojim bi se podaci vratili u njihov izvorni oblik. U P2P transakciji, podaci su u potpunosti enkriptovani od trenutka kada kupac unese svoje informacije do trenutka kada ih primi procesor plaćanja.



Slika 18 - Grafički prikaz transakcije koja je enkriptovana pomoću P2P standarda

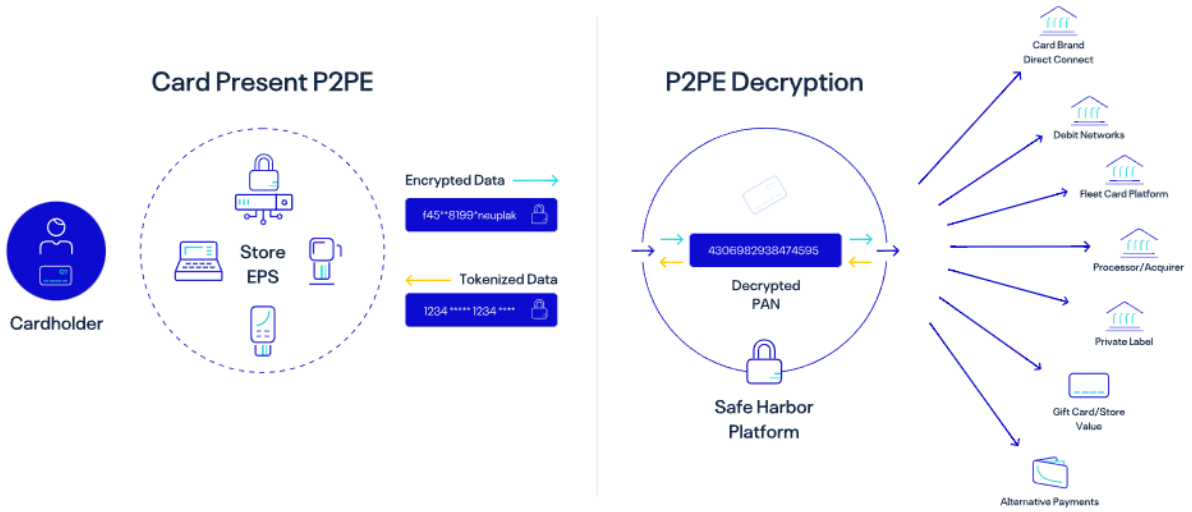
Iako koncept enkripcije postoji vijekovima, P2P enkripcija je specifičan oblik hardverske enkripcije koji se odvija putem bezbjednog uređaja za plaćanje prilagođenog svojoj svrsi. Ovi uređaji se smatraju „ojačanim“, što znači da su otporni na prijetnje i teški za provalu. P2PE je razvio Savjet za sigurnosne standarde industrije platnih kartica (PCI SSC), vodećih kompanija i učesnika u industriji plaćanja koji učestvuju u razvoju standarda i podršci za globalnu mrežu elektronskih plaćanja.

Kada vlasnik kartice obavi kupovinu na prodajnom mjestu (POS), on provlači magnetnu traku ili ubacuje čip putem uređaja za interakciju (POI), koji je obično PIN terminal za čitanje kartica proizveden od strane renomiranih proizvođača kao što su VeriFone, PAX ili Equinox.

POI uređaj se smatra sigurnosnim modulom otpornim na manipulisanje (TRSM), jer sadrži fizičke zaštite koje spriječavaju ugrožavanje bezbjednosti softvera ili hardvera. Softver za P2P enkripciju na uređaju odmah primjenjuje algoritamski izračun za enkripciju povjerljivih podataka o platnoj kartici, poput broja računa i podataka za praćenje. Ova enkripcija plaćanja obezbjeđuje da podaci ne budu izloženi čak i ako dođe do presretanja, penetracije mreže ili POS sistema.

Enkriptovani kodovi se zatim šalju payments gateway-u ili procesoru radi dekripcije unutar HSM (modula za hardversku sigurnost), koji se također naziva „sigurno utočište“. Kada se podaci

dekriptuju nazad u originalne informacije o kartici, šalju se izdavaocu kartice radi autorizacije i mogu se ponovo enkriptovati u drugi format. Banka potom odobrava ili odbija transakciju, u zavisnosti od statusa platnog računa vlasnika kartice.



Slika 19 - P2PE enkripcija i dekripcija transakcije sa tokenizacijom

Trgovac zatim dobija obavještenje o tome da li je plaćanje prihvaćeno ili odbijeno. Ovo obaveštenje može također sadržati jedinstveni referentni broj tj token koji trgovac može sačuvati. Ovi tokeni za plaćanje su posebno generisani za trgovca i koriste se za predstavljanje originalne transakcije. Trgovac može koristiti token da se pozove na transakciju ili čak da izvrši povraćaj novca kupcu, bez potrebe za informacijama o njegovoj kartici.

Validovano P2PE rješenje odnosi se na PCI-validaciju, što je potvrda da su svi uređaji, aplikacije i procesi koji se koriste za enkripciju i dekripciju podataka o plaćanju sigurni.

U osnovi, pružalac rješenja osigurava da:

- Svi podaci budu sigurno enkriptovani odmah nakon provlačenja ili ubacivanja kartice u POI uređaj, sve dok ne stignu u sigurno utočište za dekripciju.
- Sav hardver uključen u ponudu bude ojačan i sigurno upravljan.
- Svi kriptografski ključevi korišteni u procesu budu sigurno generisani, prenjeti i skladišteni.

Iako nevalidovano P2PE rješenje može koristiti istu tehnologiju kao validovano, možda neće pružati isti nivo sigurnosti. Da bi P2PE rješenje dobilo PCI validaciju, njegov pružalac i svi povezani učesnici moraju biti procjenjeni i verifikovani od strane P2PE kvalifikovanog sigurnosnog procjenjitelja (QSA), prije konačnog odobrenja od strane savjeta za sigurnosne standarde. P2PE-QSA kompanije su nezavisne treće strane koje ispunjavaju zahtjeve savjeta za

sigurnosne standarde industrije platnih kartica (PCI SSC) u pogledu obrazovanja i iskustva i koje su položile neophodni ispit.

Slika 20 - Logo "Payments Card Industry" Security Standards Council

Što se tiče zahtijeva za validaciju, P2PE rješenja moraju:

- Obezbijediti sigurnu enkripciju podataka o plaćanju unutar TRSM modula POI/terminala za plaćanje. Rješenje mora koristiti tehnologiju koja se pridržava standarda savijeta za PCI, uključujući usklađenost sa standardom Secure Reading and Exchange of Data (SRED) i upotrebu sigurnih metodologija enkripcije i svih operacija s kriptografskim ključevima.
- Omogućiti sigurno upravljanje svim uređajima za enkripciju i dekripciju, kao i okruženjem za dekripciju i svim dekriptovanim podacima o računu. Potrebno je uspostaviti skup kontrola i procesa za osiguranje integriteta P2PE rješenja, uključujući inspekcije, upravljanje lancem vlasništva i revizije.
- Ažurirati uputstvo za P2PE svaki put kada se doda novi uređaj ili promjeni proces, i to kroz propisani postupak.

Iako je P2PE visokog nivoa sigurnosti, postoje tačke ranjivosti u procesu. Budući da su podaci o kartici ne-enkriptovani između dve krajnje tačke, tj. platnog prolaza i izdavaoca kartice, postoji mogućnost da podaci budu presretnuti ili pristupljeni u procesorskoj banci. Tokenizacija može zaštititi od ovoga tako što osigurava da, kada se osjetljive informacije dekriptuju, podaci o računu i drugi lično prepoznatljivi podaci potrošača budu zamjenjeni tokenom. U tom trenutku, podaci poput broja kartice mogu se pristupiti samo putem sigurnog skladišta tokena od strane sistema koji ga je generisao. P2PE također ne može pružiti zaštitu od fizičkih pretnji, poput uređaja za krađu podataka (skimmeri i shimmeri), koji mogu biti korišteni za prikupljanje podataka sa magnetne trake ili čipa na POI terminalima. Zbog toga je inspekcija fizičkih uređaja i okruženja dio PCI validacije kako bi se obezbjedile odgovarajuće kontrole i sigurnost.

Slika 21 - Veća učestalost korištenja skimmera u svrhu krađe podataka

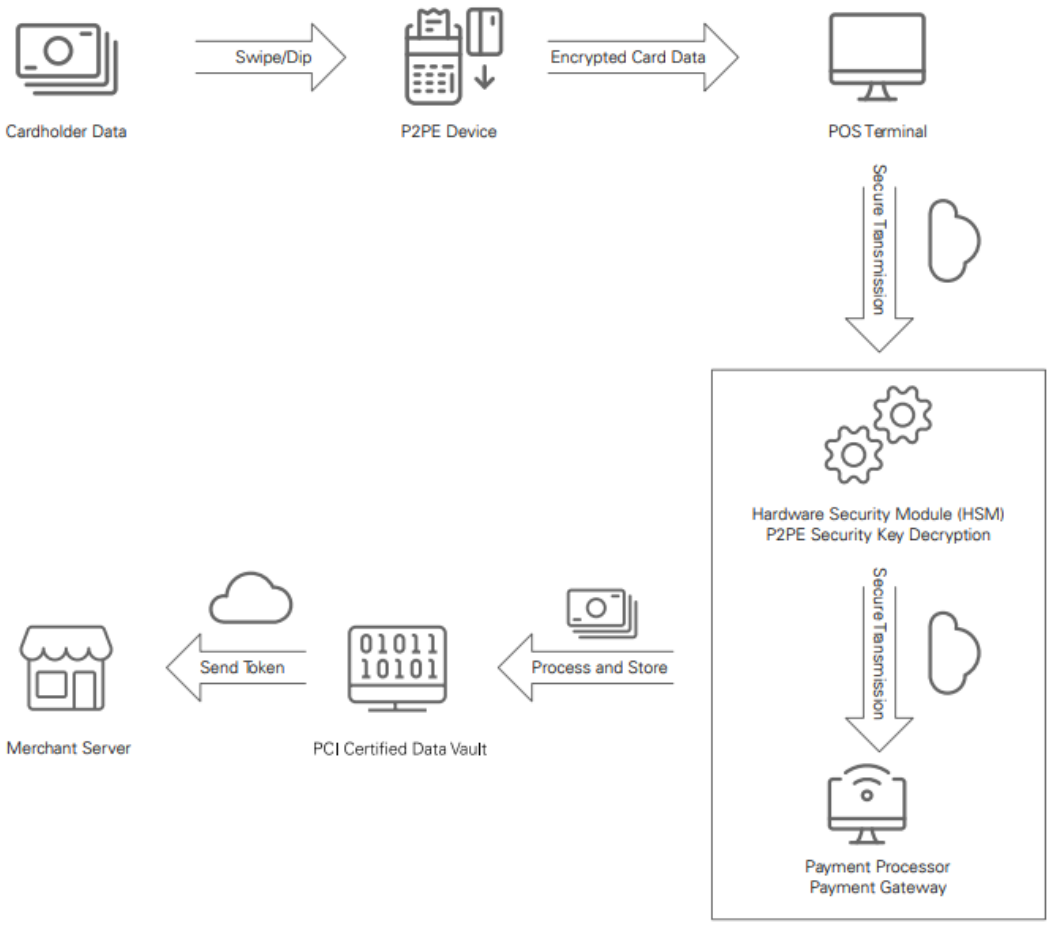
Postoje i određeni operativni zahtijevi za trgovce koji koriste P2PE:

- Poslovni subjekti moraju godišnje popunjavati SAQ P2PE kako bi postigli PCI usklađenost.
- P2PE uputstvo (PIM) mora se pažljivo pratiti i adekvatno implementirati radi ispunjavanja PCI standarda.
- Trgovci moraju voditi potpuno dokumentovan zapis svih aktivnosti koje osiguravaju terminale za plaćanje unutar svoje prodavnice.
- Kupci moraju obaviti nekoliko revizija godišnje kako bi osigurali usklađenost sa PIM-om.

Međutim, ovi zahtijevi predstavljaju manje neugodnosti u poređenju sa prednostima koje pružaju P2PE rješenja“ [15].

3.1.1. P2PE tok podataka (engl. Data flow)

“Tok podataka u P2PE rješenju uključuje sigurno enkriptovanje podataka o kartici na tački interakcije (POI), nakon čega podaci putuju kroz payments gatewaz. Podaci se dekriptuju na sigurnom mestu, a zatim šalju banci na autorizaciju. Tokenizacija se može koristiti kako bi osjetljivi podaci bili zamjenjeni tokenima koji nisu osjetljivi“ [16].



Slika 22 - Dijagram toka u P2PE rješenju

3.1.2. Benefiti P2PE solucije

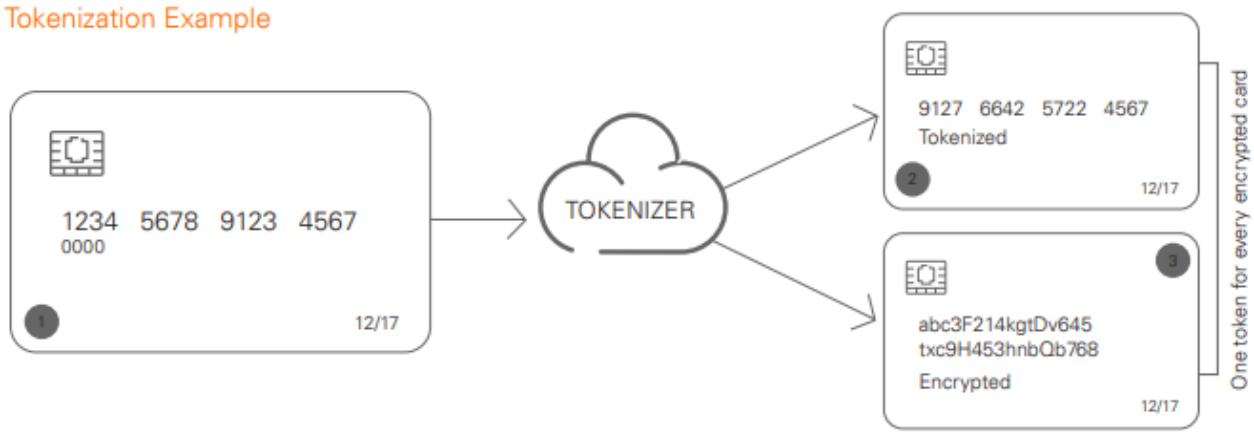
„Trgovci koji koriste PCI-P2PE validirana rješenja imaju pojednostavljene napore za usklađivanje, jer su podložni manjim zahtjevima PCI DSS. Ovo može značajno uštedjeti vrijeme i novac, jer su zahtjevi za PCI znatno smanjeni. Organizacije koje koriste P2PE rješenje mogu da završe kraći PCI samoprocjeni upitnik, sa smanjenim brojem pitanja, sa 329 (SAQ-D) na samo 35 (P2PE-HW). Također, P2PE rješenje štiti poslovanje u slučaju prevare, jer je pružalac rješenja odgovoran za gubitak podataka i kazne koje mogu biti izrečene od strane kartičnih brendova (Amex, Visa, Mastercard, Discover i JCB)“ [16].

3.2. Tokenizacija (engl. Tokenization)

„Tokenizacija se često miješa sa P2PE, jer oba rješenja uključuju konvertovanje osjetljivih podataka u podatke koji su beskorisni hakerima. Tokenizacija i P2PE su različite tehnologije koje služe različitim svrhama unutar trgovinskog okruženja“ [16].

„Kao što je prethodno objašnjeno, P2PE rješenje se koristi za zaštitu podataka sa kreditnih kartica dok podaci putuju od POI-a do zaštićenog okruženja provajdera rješenja. P2PE rješenje se obično kombinuje sa tokenizacijom kako bi se proizveo nasumično generisani broj koji predstavlja platnu karticu. Dužina i format tokena variraju zavisno od provajdera rješenja“ [16].

„Ovaj nasumično generisani broj može se ponovo koristiti od strane preduzeća za obradu buduće transakcije putem platnog sistema provajdera. Token ne sadrži podatke o kreditnoj kartici, nije vrijednost koja se može dekriptovati i vraćena u originalni broj kreditne kartice (samo provajder rješenja može regenerisati originalni broj kartice – uz neke izuzetke gdje trgovac može dekriptovati tokene) i ne može se koristiti van platnog sistema provajdera“ [16].



Slika 23 - Primjer tokenizacije debitne ili kreditne kartice

„Kreditni kartični tokeni obično prikazuju posljednje četiri cifre kreditne kartice, ali mogu uključivati i prve dvije ili šest cifara (BIN broj) kartice. Pošto token ne sadrži osjetljive podatke, preduzeće može da čuva token bez obaveze stalne PCI usklađenosti u vezi sa čuvanjem podataka o vlasniku kartice“ [16].

3.3. PCI DSS standard

Kreditne kartice danas predstavljaju nezaobilazan alat u finansijskim transakcijama, a njihova popularnost u online plaćanjima bilježi značajan rast. Prema podacima iz prethodne godine, broj vlasnika kreditnih kartica premašio je 3 milijarde. Prodaja putem interneta dostigla je vrijednost od 33,9 milijardi dolara u posljednjem kvartalu 2006. godine, što je za 25% više nego u istom periodu 2005. godine.

Međutim, sa širenjem e-trgovine dolazi i do porasta prevara i krađa. Krađe putem kreditnih kartica, koje podrazumjevaju neovlašteno korištenje tuđih podataka, činile su 26% svih slučajeva krađe identiteta u 2005. godini. Te iste godine, finansijske institucije pretrpjele su gubitke veće od 48 milijardi dolara, dok su privatna lica izgubila preko 5 milijardi dolara zbog ovakvih prevara. Ovi podaci ukazuju na značajan finansijski uticaj prevara na globalnom nivou.

Slika 24 - Grafički prikaz prevara i krađe putem kreditnih kartica od 2010 do 2020

Jedan od najpoznatijih slučajeva krađe kartičnih podataka dogodio se 17. januara 2007. godine, kada je kompanija TJX Companies Inc. objavila da je njen sistem za obradu plaćanja kreditnim i debitnim karticama hakovan. Napad je rezultirao krađom podataka 45,7 miliona korisnika, uključujući informacije o brojevima kartica i oko 455.000 zapisa o povratima robe, koji su sadržavali imena i brojeve vozačkih dozvola korisnika. Ovaj incident se smatra jednim od najvećih hakerskih napada na kartične sisteme.

Kako bi odgovorile na sve češće slučajeve računarskog kriminala i prevara, vodeće kartične kompanije udružile su snage i uspostavile jedinstveni sigurnosni standard - PCI DSS (Payment Card Industry Data Security Standard). Ovaj standard postavlja smjernice za bezbjednu obradu, skladištenje i prenos podataka o plaćanju karticama.

PCI DSS ima ključnu ulogu u radu pružaoca usluga plaćanja, jer se od svih organizacija koje upravljaju kartičnim podacima zahtijeva usklađenost sa njegovim pravilima. Time se štite korisnici, smanjuju rizici od prevara i osigurava bezbjednost finansijskih transakcija u savremenom digitalnom okruženju.

Ovaj standard ne samo da definiše tehničke i operativne zahtjeve, već podstiče i kontinuiranu edukaciju zaposlenih o bezbjednosnim praksama. Njegova implementacija je ključna za povjerenje korisnika i održavanje stabilnosti u industriji plaćanja.

PCI DSS predstavlja sveobuhvatan skup pravila i procedura osmišljenih da osiguraju bezbjednost kreditnih, debitnih i drugih kartičnih transakcija, pružajući zaštitu vlasnicima kartica od zloupotrebe njihovih ličnih podataka. Standard je razvijen 2004. godine kroz saradnju vodećih kompanija u kartičnom poslovanju kao što su Visa, MasterCard, Discover i American Express. Ove kompanije, zajedno sa japanskom kompanijom JCB, formiraju PCI odbor za sigurnosne standarde (PCI SSC), koji upravlja i unapređuje PCI DSS standard.

Primarni cilj odbora jeste da podrži organizacije koje se bave obradom kartičnih plaćanja, smanjujući rizik od prevara i kompromitovanja podataka. PCI DSS postavlja smjernice za provjeru, obradu i zaštitu kartičnih informacija, sa posebnim fokusom na smanjenje izloženosti korisničkih podataka potencijalnim prijetnjama.

Ovaj standard je obavezan za sve organizacije koje čuvaju, obrađuju ili prenose podatke o karticama koje nose logo bilo kojeg od navedenih kartičnih brendova. Njegova implementacija ne samo da štiti podatke korisnika već i pomaže u jačanju povjerenja između pružalaca usluga i njihovih klijenata.

Provjera usklađenosti sa PCI DSS standardom sprovodi se na različite načine, u zavisnosti od obima transakcija koje organizacija obrađuje. Kompanije sa velikim brojem transakcija prolaze godišnju procjenu koju vrši kvalifikovani procjenitelj sigurnosti (engl. Qualified Security Assessor, QSA). S druge strane, organizacije sa manjim obimom transakcija koriste upitnik za samoprocjenu (engl. Self-Assessment Questionnaire, SAQ) kako bi samostalno procjenile svoje usklađivanje sa zahtjevima standarda.

Vanjsko skeniranje mreže, koji je dio ovih provjera, mora obaviti ovlašteni dobavljač aplikacija za skeniranje (engl. Approved Scanning Vendor, ASV). Ovi dobavljači su stručnjaci za informacionu sigurnost, specijalizovani za pružanje rješenja koja identifikuju ranjivosti u mrežama i sistemima kompanija. Da bi dobili sertifikat od PCI odbora za sigurnosne standarde, ASV dobavljači moraju svake godine prolaziti rigorozne testove. Nakon sertifikacije, oni su ovlašćeni da sprovode skeniranja neophodna za usklađivanje sa PCI DSS standardom.

Kvalifikovani procjenjitelji sigurnosti (QSA) su sertifikovani konsultanti za informacionu bezbjednost, obučeni od strane PCI odbora za sigurnosne standarde. Njihova uloga uključuje obavljanje provjera na lokaciji klijenata kako bi se osiguralo da su svi aspekti poslovanja usklađeni sa PCI DSS pravilima. Također, QSA procjenjitelji nadgledaju kvartalna skeniranja ranjivosti koje obavljaju ASV dobavljači, čime se dodatno potvrđuje bezbjednost mreža i sistema.

Dio PCI DSS standarda uključuje zahtijeve za sigurnost PIN transakcija (engl. Point-to-point credit card encryption, PTS). Ovi zahtijevi se odnose na proizvođače uređaja koji se koriste za obradu PIN kodova korisnika i drugih kartičnih aktivnosti. Proizvođačima se pružaju smhernice o dizajniranju, proizvodnji i transportu uređaja do organizacija koje ih koriste, kako bi se osigurala potpuna zaštita podataka korisnika.

Šifriranje P2PE pruža zaštitu kartičnih podataka čak i u slučaju krađe kartice, neovlaštenog pristupa sistemima za plaćanje ili dok su podaci u prenosu prema kartičnom procesoru. Moderni uređaji obavljaju šifriranje podataka pre nego što transakcija započne, čime trgovci nemaju pristup nešifrovanim informacijama korisnika. Ovi uređaji koriste Triple DES algoritam za šifriranje i DUKPT ključeve kako bi osigurali zaštitu i bezbjedan prenos podataka putem bilo koje mreže.

Još jedan način zaštite podataka je primjena tokenizacije. Tokeni su generisane vrijednosti koje mogu imitirati originalne osjetljive podatke, poput broja kartice (Primary Account Number, PAN). Na primjer, token može biti iste dužine kao broj kartice ili zadržavati posljednje četiri cifre originalnog broja. Kada se traži autorizacija transakcije, trgovac dobija token umijesto stvarnog broja kartice, zajedno sa autorizacionim kodom. Tokeni se skladište u zaštićenim sistemima, odvojenim od stvarnih podataka o vlasniku kartice.

Primjena tokenizacije smanjuje rizik od zloupotrebe, jer napadači ne mogu lako pristupiti podacima izvan sistema za skladištenje tokena. Također, tokenizacija može pojednostaviti zahtijeve PCI DSS standarda jer sistemi koji ne skladište niti obrađuju osetljive podatke mogu biti isključeni iz PCI DSS revizija.

Slika 25 - Kartični brendovi koji su osnovali PCI DSS odbor

Standard sigurnosti aplikacija industrije platnih kartica (engl. Payment Application Data Security Standard, PA-DSS) odnosi se na organizacije koje razvijaju softverska rješenja ili integrišu aplikacije za obradu kartičnih transakcija. Ovaj standard postavlja smjernice za zaštitu podataka o korisnicima kartica u softverima koji se koriste za skladištenje, obradu ili prenos informacija tokom procesa autorizacije transakcija.

PA-DSS standard se primjenjuje na softverska rješenja koja se prodaju, distribuiraju ili licenciraju trećim stranama. Njegova svrha je osiguranje da aplikacije budu dizajnirane i razvijene na način koji minimalizuje rizike od neovlaštenog pristupa i kršenja podataka korisnika kartica.

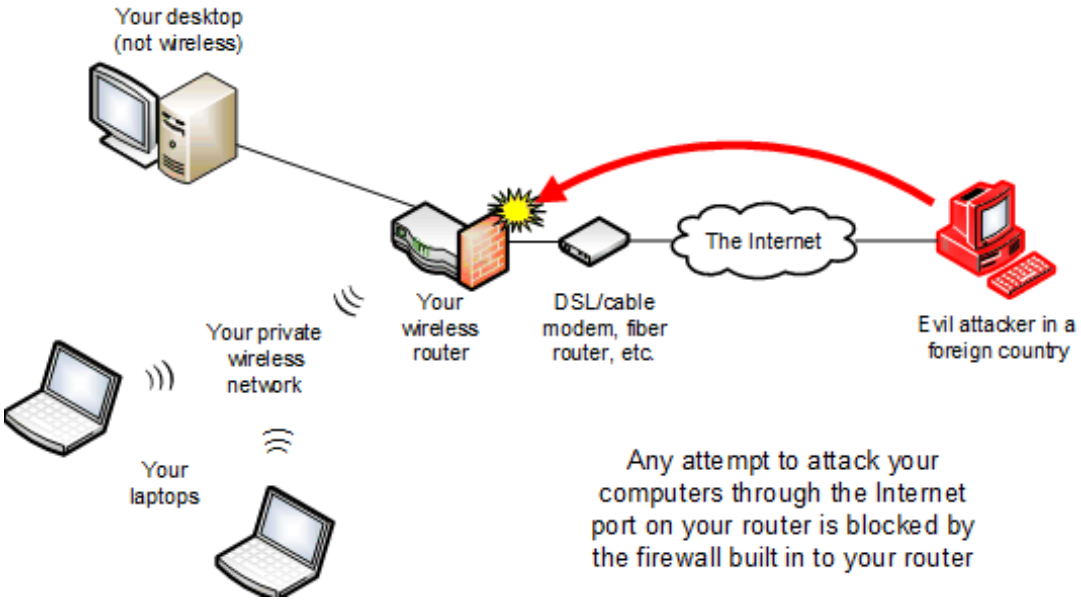
Organizacije koje usklade svoja rješenja sa PA-DSS standardom ne samo da povećavaju povjerenje korisnika već i pomažu svojim klijentima u ispunjavanju zahtijeva PCI DSS standarda, obezbjeđujući time sigurnost u cijelokupnom lancu kartičnih transakcija.

3.3.1. Izgradnja i održavanje sigurnosne mrežne infrastrukture

Za obavljanje sigurnih kartičnih transakcija neophodno je uspostaviti i održavati sigurnu mrežnu infrastrukturu. Ovo uključuje primjenu tehničkih i organizacionih mjera kako bi se zaštitili podaci o korisnicima.

- Implementirati i redovno održavati firewall konfigurisan za zaštitu kartičnih podataka.
- Izbjegavati upotrebu fabrički postavljenih lozinki i sigurnosnih parametara koje dobavljači hardvera i softvera pružaju uz proizvode.

Firewall igra ključnu ulogu u zaštiti mreže. Oni moraju biti dovoljno snažni da obezbjede efikasnu zaštitu, a da pritom ne ometaju poslovne procese. Posebno su važni firewall-i za bežične mreže (Wireless LAN), koje su podložne prisluškivanju i napadima zlonamjernih korisnika.



Slika 26 - Uloga Firewall-a na Wireless LAN mreži

Osim Firewall-a, posebna pažnja se posvećuje bezbjednosti autorizacionih podataka, kao što su PIN-ovi i lozinke. Ove informacije ne smiju biti uključene u standardne postavke uređaja i aplikacija koje dolaze od dobavljača. Kupci moraju imati mogućnost da lako i redovno mjenjaju ovakve podatke kako bi dodatno smanjili rizik od neovlaštenog pristupa.

3.3.2. Zaštita kartičnih podataka

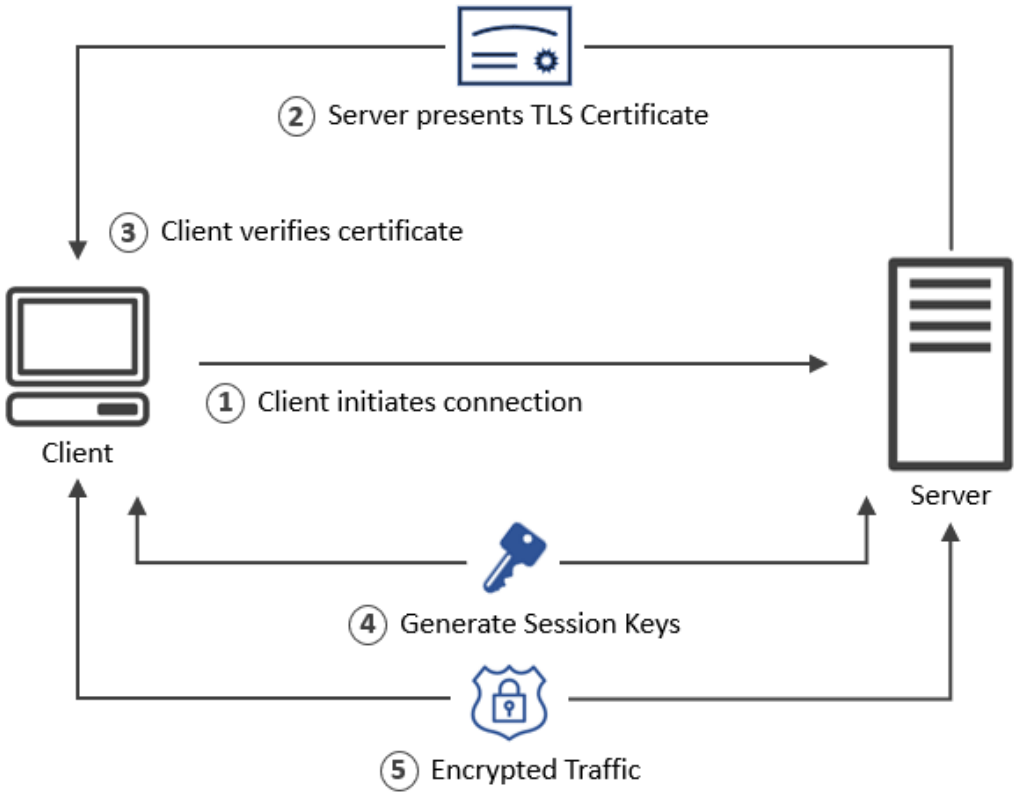
Podaci vlasnika kartica moraju biti zaštićeni u svakom trenutku, bilo da su pohranjeni ili preneseni preko mreža.

- Osigurati zaštitu pohranjenih kartičnih podataka
- Šifrovati kartične podatke tokom prenosa preko otvorenih i javnih mreža

Skladištenje osjetljivih podataka, kao što su datumi rođenja, matični brojevi, brojevi ličnih dokumenata, brojevi telefona i e-mail adrese, mora biti zaštićeno od neovlaštenog pristupa. Repozitorijumi koji sadrže ove informacije moraju imati ugrađene mehanizme zaštite kako bi se minimizovali rizici od krađe podataka.

Tokom prenosa kartičnih informacija putem javnih mreža, šifrovanje je obavezno kako bi se podaci učinili nedostupnim potencijalnim napadačima. Digitalno šifrovanje je od presudne važnosti, posebno u kontekstu e-trgovine, gdje transakcije često uključuju prenos osjetljivih informacija preko interneta.

Upotreba modernih šifrovnih metoda, poput **TLS (Transport Layer Security)**, ključna je za osiguranje da prenijeti podaci ostanu zaštićeni, čime se osigurava povjerenje korisnika u platne sisteme. Poštovanje ovih zahtijeva smanjuje rizik od kršenja podataka i pomaže organizacijama u ispunjavanju PCI DSS standarda.



Slika 27 - Grafički prikaz Transport Layer Security TSL metode šifrovanja podataka

3.3.3. Održavanje programa za upravljanje ranjivostima

Zaštita sistema od zlonamjernih napadača postiže se korištenjem ažuriranih antivirusnih i antimalware rješenja, kao i drugim sigurnosnim alatima koji mogu spriječiti napade.

- Korištenje i redovno ažuriranje antivirusnih programa
- Razvijanje i održavanje sigurnih sistema i aplikacija

Softverske prijave moraju biti oslobođene grešaka i ranjivosti koje bi mogle omogućiti eksploataciju osjetljivih podataka, što bi moglo dovesti do njihovog neovlaštenog pristupa, krađe ili izmjene. Ovo uključuje rigoroznu kontrolu kvaliteta i testiranje aplikacija prije nego što budu implementirane u produkciju.

Redovno ažuriranje antivirusnih alata i softverskih rješenja koje preporučuju proizvođači ključno je za osiguranje maksimalnog nivoa zaštite. Posebno je važno koristiti bezbjednosne zakrpe i nadogradnje operativnih sistema kako bi se zaštitili od novih prijetnji koje se stalno razvijaju.

Slika 28 - Pouzdani Antivirus softveri koji se mogu koristiti u zaštiti transakcija

Osim antivirusnih rješenja, treba koristiti i alat za praćenje ranjivosti i proaktivno identifikovati potencijalne slabosti. Implementacija sigurnosnih procedura za brzo rješavanje novih ranjivosti dodatno unapređuje otpornost sistema na cyber prjetnje.

Slika 29 - Potreba za redovnim ažuriranjem Windows operativnog sistema i Windows Defender-a

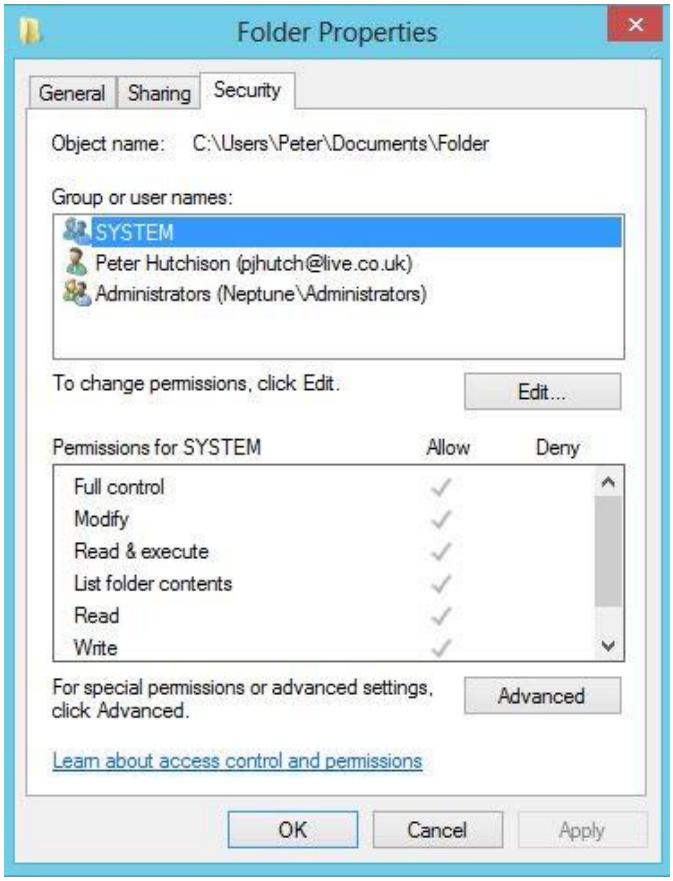
3.3.4. Implementacija jakih provjera pristupa

Pristup podacima i operacijama sistema mora biti strogo kontrolisan i verifikovan kako bi se smanjio rizik od zloupotrebe.

- Ograničiti pristup kartičnim podacima kroz pažljivo modeliranje poslovnog procesa
- Dodijeliti jedinstveni ID svakom korisniku koji pristupa računaru
- Ograničiti fizički pristup kartičnim podacima

Vlasnici kartica trebaju biti oprezni u davanju podataka o kartici, pružajući ih samo onim organizacijama koje zaista moraju imati te informacije kako bi obavile sigurnu i učinkovitu transakciju. Svaka osoba koja pristupa računarskom sistemu kartičnog poslovanja mora imati jedinstveni identifikacijski broj, korisničko ime ili lozinku kako bi se obezbjedio sigurnosni trag i spriječila zloupotreba.

Kartični podaci moraju biti zaštićeni ne samo elektronski, već i fizički. Primjeri fizičke zaštite uključuju korištenje uređaja za uništavanje dokumenata, izbjegavanje nepotrebno kopiranja papirnih podataka te korištenje sigurnosnih ključeva ili brava na kantama za smeće, kako bi se spriječile moguće krađe podataka iz odbačenih materijala.



Slika 30 - Podešavanje User Permission-a unutar Windows-a

3.3.5. Usklađivanje sa standardom PCI DSS

Najveće kartične kompanije (Visa, MasterCard, American Express, Discover i JCB) zahtijevaju od organizacija koje obrađuju, skladište ili prenose kartične podatke da se usklade sa PCI DSS standardom. To uključuje banke, pružaoce usluga plaćanja i trgovce, bilo da se radi o online ili fizičkim prodajnim mjestima.

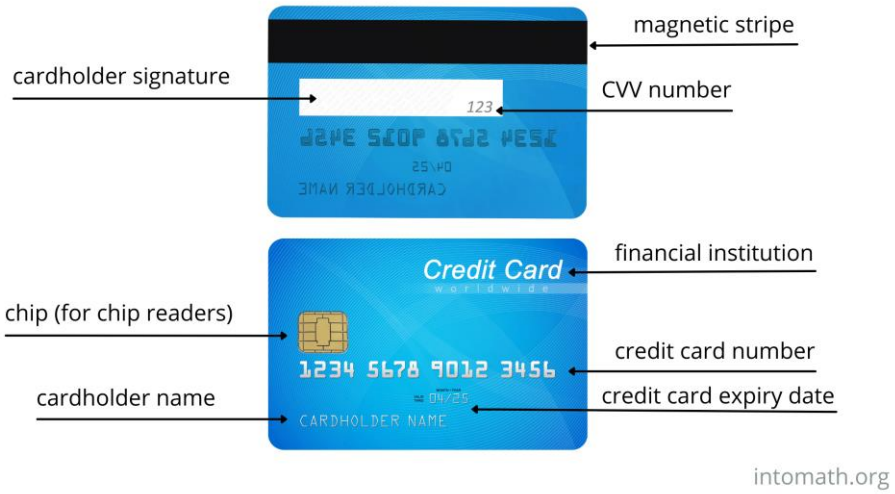
Iako je usklađenost sa PCI DSS potrebna za sve strane u procesu, formalna verifikacija nije obavezna za sve subjekte. Banke koje izdaju kartice nisu obavezne da prolaze kroz PCI DSS verifikaciju, ali ako dođe do sigurnosnog incidenta, oni koji nisu usklađeni sa standardom mogu se suočiti sa sankcijama, uključujući novčane kazne.

Usklađenost nije jednokratan proces. Trgovci i drugi subjekti moraju godišnje provjeravati svoju usklađenost i održavati je tokom godine. U zavisnosti od veličine organizacije, može se zahtijevati samo samoprocjena putem upitnika (SAQ) ili formalna procjena na lokaciji, koju obavlja kvalifikovani procjenitelj. Također, za organizacije koje prenose kartične podatke putem interneta, potrebno je kvartalno skeniranje mreže zbog ranjivosti.

Trgovci i druge organizacije moraju svojim bankama dostaviti potvrdu o usklađenosti (AOC), a u nekim slučajevima dodatne izvještaje o skeniranju mreže ili godišnje potvrde o procjeni na lokaciji.

Usklađenost mora biti održavana svakodnevno, a godišnja verifikacija je obavezna za trgovce sa više od 6 miliona transakcija godišnje, kao i za većinu banaka. Manji trgovci mogu koristiti upitnik za samoprocjenu, umjesto prolaska kroz procjenu na lokaciji.

Najčešći razlog neuspijeha u usklađivanju sa PCI DSS je neadekvatna zaštita podataka, kao što je čuvanje CVV2/CVC2 ili PIN brojeva nakon autorizacije. Cilj PCI DSS-a je povećanje sigurnosti platnih transakcija, čime se smanjuje rizik od zloupotrebe, a sve to može se postići bez velikih ulaganja u složene sigurnosne sisteme.



Slika 31 - Sadržaj modernih kreditnih i debitnih kartica

3.3.6. Prednosti usklađivanja sa PCI DSS standardom

Iako se na prvi pogled usklađivanje sa PCI DSS standardom može činiti nepotrebnim, posebno manjim organizacijama, dugoročne prednosti su značajne, posebno za one koje žele unaprijediti svoje poslovanje.

Usklađenost sa sigurnosnim standardima pruža mnoge koristi, uključujući:

- **Povećanje povjerenja kupaca** - usklađenost znači da su sistemi sigurni, što korisnicima omogućava da sigurno obavljaju transakcije sa svojim karticama
- **Bolja pripremljenost za druge propise** - organizacije koje se usklade sa PCI DSS standardom često budu bolje pripremljene za usklađivanje s drugim zakonodavnim aktima kao što su HIPAA ili SOX
- **Jačanje korporativnih sigurnosnih strategija** - postavljanje temelja za dalji razvoj sigurnosnih politika i infrastrukture
- **Poboljšanje IT efikasnosti** - mogućnost za optimizaciju IT sistema kroz sigurnosne protokole

S druge strane, neusklađenost sa PCI DSS može imati ozbiljne posljedice:

- **Oštećenje ugleda i poslovanja** - jedan sigurnosni incident može trajno ugroziti reputaciju organizacije i sposobnost za efikasno poslovanje
- **Posljedice za potrošače i institucije** - kompromitovani podaci mogu ozbiljno uticati na potrošače, trgovce i finansijske institucije, dok neovlašteni pristup podacima može dovesti do katastrofalnih gubitaka
- **Pravne i finansijske posljedice** - moguće posljedice uključuju tužbe, gubitak osiguranja, otkazivanje računa, kazne od izdavača kartica i državne kazne

Usklađenost ne samo da štiti podatke, već i doprinosi izgradnji povjerenja sa kupcima. Kada se kupci uvjere u sigurnost transakcija, veća je vjerovatnoća da će se vratiti i preporučiti organizaciju drugima.

Organizacije koje se usklade sa PCI DSS standardima također uživaju bolji ugled među partnerima, uključujući banke i pružaoce usluga plaćanja, što omogućava širenje poslovanja.

Kroz stalnu adaptaciju i praćenje novih prijetnji, PCI DSS pomaže organizacijama da se održe sigurnima u svijetu koji se brzo mjenja. Kako napadi postaju sofisticiraniji, organizacije koje se usklade sa standardom čine dio globalnog sistema zaštite kartičnih podataka.

3.3.7. Podjela pružatelja usluga

Od verzije 1.2 PCI DSS standarda, pružatelji usluga koji sudjeluju u obradi kartičnih podataka, bilo direktno ili indirektno, podliježu različitim zahtjevima usklađenosti. To uključuje organizacije koje obrađuju, prenose ili pohranjuju kartične podatke, kao i one koji održavaju mrežnu opremu ili aplikacije povezane sa PCI DSS-om.

Nivo 1, ovaj nivo obuhvata:

- Banke, procesore za plaćanja, sisteme za internet naplatu (Internet Payment Gateway)
- Trgovce sa više od 600,000 transakcija VISA kartica godišnje

Subjekti u ovoj grupi obavezni su:

- Obaviti godišnju PCI DSS provjeru koju vrši ovlašteni revizor odobren od strane PCI DSS odbora
- Redovno skeniranje mreže svaka tri mjeseca
- Penetracioni test jednom godišnje

Nivo 2, ovaj nivo obuhvata:

- Subjekte koji pohranjuju, obrađuju ili prenose kartične podatke s 120,000 do 600,000 transakcija godišnje

Subjekti u ovoj grupi obavezni su:

- Obaviti godišnji atest koji se predaje banci s kojom imaju ugovor
- Skenirati mrežu svaka tri mjeseca

Nivo 3, ovaj nivo obuhvata:

- Subjekte koji pohranjuju, obrađuju ili prenose kartične podatke, ali imaju manje od 120,000 transakcija godišnje

Subjekti u ovoj grupi obavezni su:

- Obaviti godišnji atest koji se predaje banci s kojom imaju ugovor

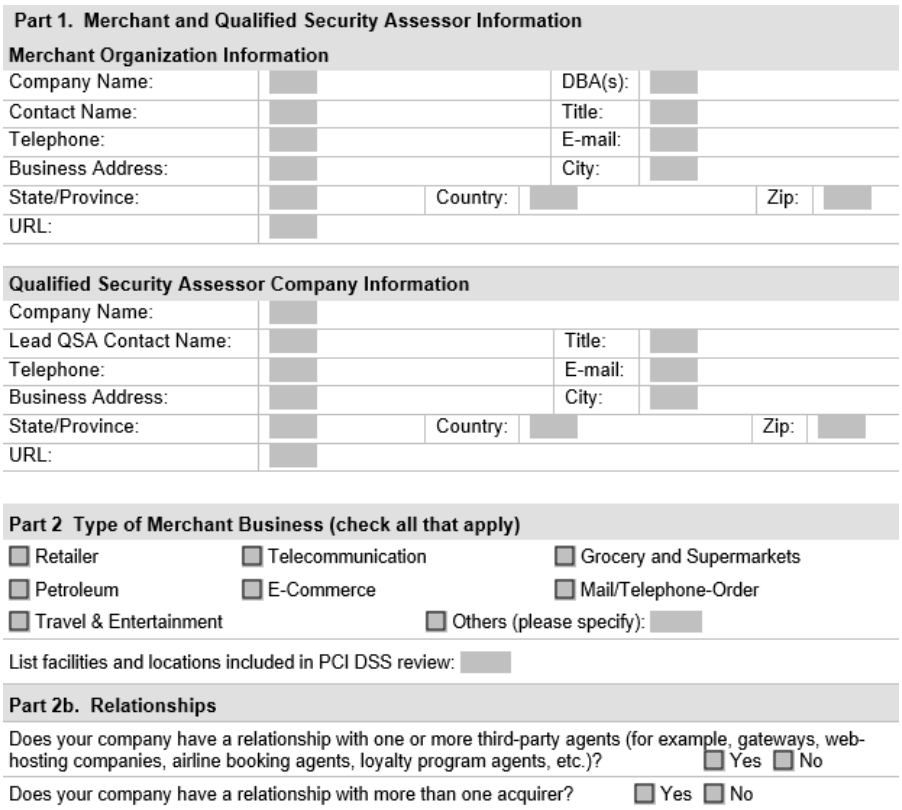
Razlike u nivoima pružatelja usluga temelje se na broju transakcija koje obrada podrazumijeva, čime se određuju zahtjevi za sigurnosne provjere i izvještavanje.

3.4. Atest o usklađenosti (engl. Attestation of Compliance)

Atest o usklađenosti (AOC) je ključan dokument u procesu sigurnoshih audita, a posebno u standardima kao što je PCI DSS (engl. Payments Card Industry Data Security Standard). Ovaj dokument služi kao formalna potvdra da je organizacija prošla potrebne procese i da je usklađena sa svim sigurnosnim zahtjevima koji se odnose na zaštitu osjetljivih podataka.

AOC također pruža povjerenje svim uključenim stranama, sve od banaka, procesora plaćanja, pa sve do samih korisnika tako da organizacija održava visok nivo sigurnosti. Njegova svrha nije samo administrativna već i praktična, jer osigurava da su implementirane procedure efikasne u zaštiti podataka i znatno utiče na minimiziranje rizika od zloupotreba.

Pored ostalih prednosti, posjedovanje važećeg AOC-a značajno se povećava povjerenje klijenata i poslovnih partnera, jer pokazuje da organizacija ozbiljno shvata sigurnost podataka i implementira odgovarajuće protokole. AOC također osigurava transparentnost u procesu sigurnosnog audita, jer dokumentuje da organizacija prati jasno definisane sigurnosne standarde.



Part 1. Merchant and Qualified Security Assessor Information

Merchant Organization Information

Company Name:			DBA(s):		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Qualified Security Assessor Company Information

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2 Type of Merchant Business (check all that apply)

☐ Retailer ☐ Telecommunication ☐ Grocery and Supermarkets

☐ Petroleum ☐ E-Commerce ☐ Mail/Telephone-Order

☐ Travel & Entertainment ☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? ☐ Yes ☐ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☐ No

Slika 32 - Primjer jedne stranice iz dokumenta PCI AOC

Također, AOC omogućava pravni okvir koji može smanjiti pravne i finansijske posljedice u slučaju narušavanja sigurnosti. AOC pomaže organizacijama da identifikuju potencijalne slabosti u svojim sigurnosnim sistemima, što im omogućava da unaprijede postojeće kontrole i smanje rizik od eventualnih napada. Na ovaj način, AOC ne samo da osigurava usklađenost sa sigurnosnim standardima, već doprinosi jačanju povjerenja i kontinuiranom unapređenju sigurnosne infrastrukture organizacije.

4. Administracija sistema za plaćanje

Administracija sistema za plaćanje obuhvata ključne zadatke poput upravljanja uređajima, redovnog ažuriranja softvera kako bi se osigurala sigurnost i funkcionalnost, te kontinuiranog monitorisanja rada sistema. Korištenje alata kao što su Splunk ili Syslog omogućava praćenje događaja, analiza logova i identifikaciju potencijalnih problema u radu sistema. Proces integracije uključuje dodavanje novih uređaja, kao što su POS terminali, i kreiranje korisničkih naloga, uz osiguranje da svi elementi sistema funkcionišu u skladu sa bezbjednosnim standardima i poslovnim zahtijevima korisnika.

4.1. Instalacija i održavanje hardvera

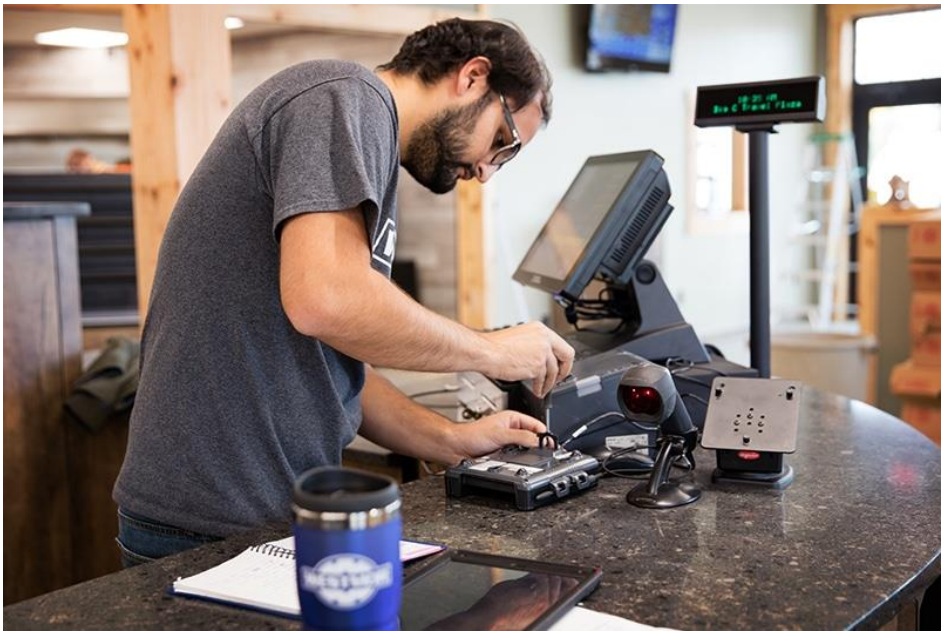
POS terminali, čitači kartica, mrežni uređaji i serveri zahtijevaju preciznu i temeljnu instalaciju kako bi sistem funkcionisao optimalno i bio bezbjedan od potencijalnih prijetnji. Proces uključuje fizičko povezivanje uređaja sa mrežom, kao i njihovu konfiguraciju kako bi omogućili nesmetan protok podataka. Ovo podrazumjeva dodjeljivanje mrežnih adresa, sinhronizaciju sa centralnim serverima i postavljanje parametara za komunikaciju putem sigurnih protokola kao što su HTTPS, TLS ili VPN.

Osim mrežnog povezivanja, svaki uređaj mora biti integrisan u postojeću infrastrukturu kako bi se omogućila kompatibilnost sa softverskim rješenjima koja upravljaju transakcijama. Postavljanje sigurnosnih parametara obuhvata instalaciju sertifikata, podešavanje enkripcije za zaštitu osjetljivih podataka i konfigurisanje pristupnih prava za korisnike i administratore.

Održavanje sigurnosti je ključni aspekt instalacije. Ovo uključuje implementaciju firewall pravila za sprečavanje neovlaštenog pristupa, kao i redovne provjere i ažuriranja firmvera (engl. firmware) kako bi se uređaji zaštitili od novih prijetnji. Serveri, kao centralne komponente sistema, zahtjevaju dodatnu pažnju pri konfigurisanju kako bi se obezbjedila stabilnost u obradi velikog broja transakcija i smanjila mogućnost zastoja.

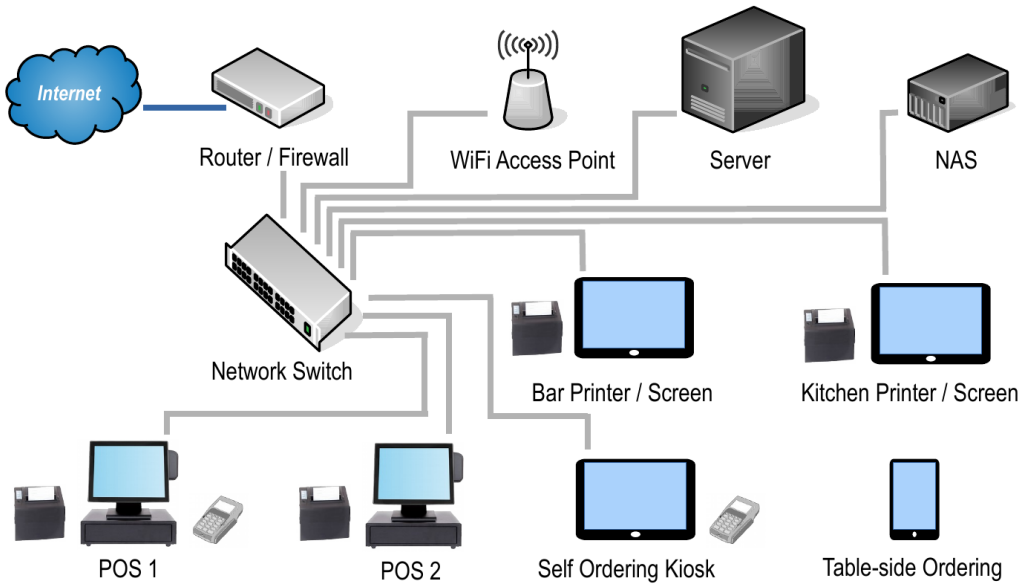
4.1.1. Instalacija POS terminala

Prvi korak u instalaciji POS terminala je njegovo fizičko postavljanje na željeno mjesto u poslovnom prostoru.



Slika 33 - Prikaz tehničara koji instalira POS Terminal sa njegovim komponentama kao što su čitač kartica i printer

Uređaj se povezuje sa napajanjem i ukoliko koristi kablovsku mrežu sa Ethernet kablom. Za bežične modele, neophodno je uspostaviti Wi-Fi vezu prema prethodno podešenoj mreži.



Slika 34 - Grafički prikaz mrežne arhitekture modernih POS Terminala (sistema)

4.1.2. Instalacija i održavanje čitača kartica

Instalacija čitača kartica zavisi od vrste konekcije koju uređaj koristi, a najčešći tipovi su Powered USB, External Powered i Ethernet konekcija.

Powered USB čitači kartica koriste USB port za napajanje i prenos podataka. Instalacija ovog tipa uređaja je jednostavna i obično uključuje povezivanje čitača sa računarom ili POS terminalom putem USB kabla.

Slika 35 - Powered USB kabal koji se koristi za prenos podataka i napajanje čitača kartica

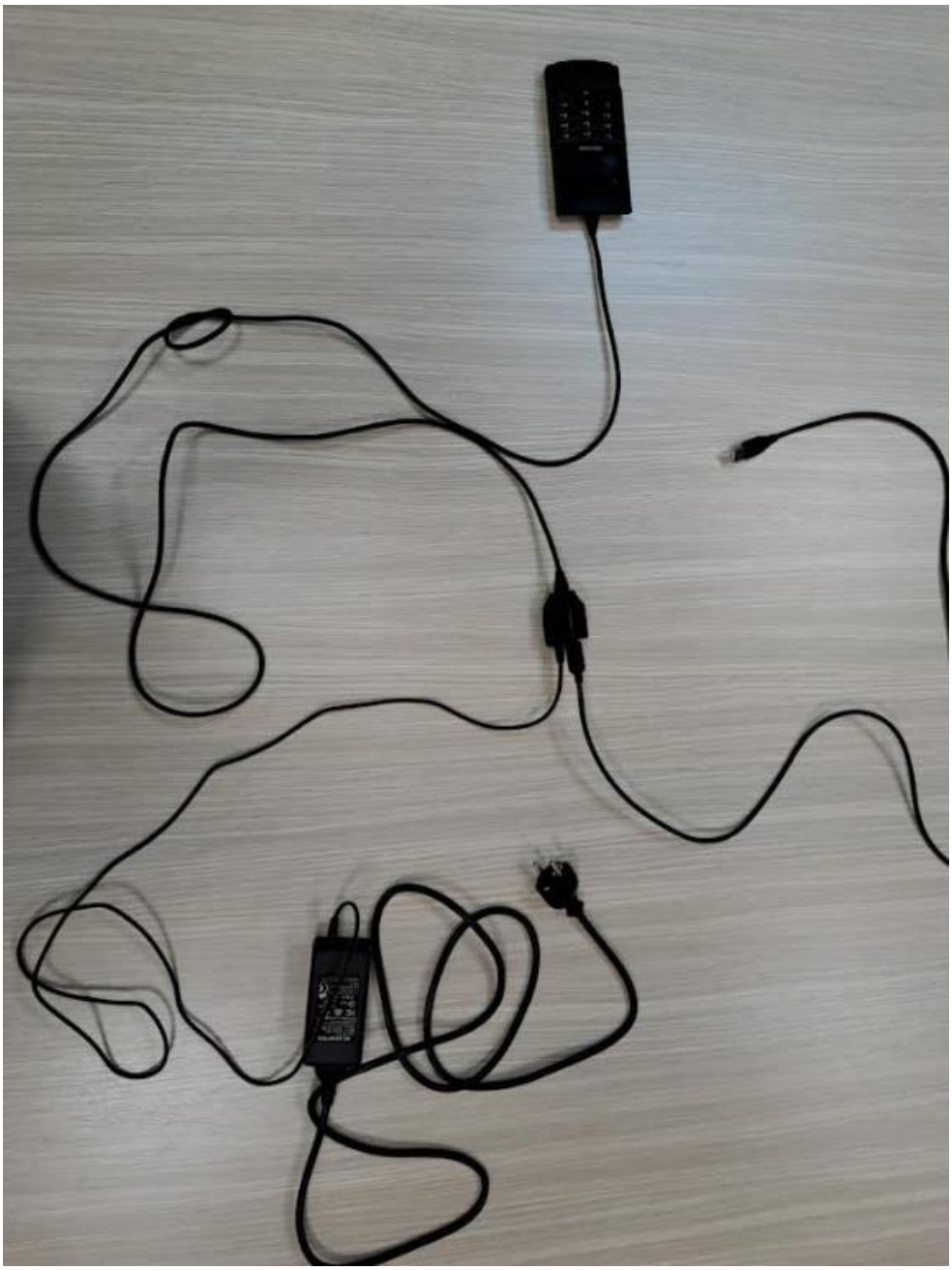
Uređaj se automatski prepoznaje od strane sistema, ali može biti potrebno instalirati odgovarajući drajver kako bi čitač mogao ispravno da komunicira sa softverom za obradu transakcija. Ovi čitači često ne zahtijevaju dodatno napajanje jer koriste napajanje sa USB porta.

Slika 36 - Čitač kartica kompanije Verifone koji koristi Powered USB prenos podataka i napajanje

External Powered čitači kartica zahtjevaju dodatni izvor napajanja, obično putem adaptera ili direktnog napajanja iz utičnice. Instalacija ovog uređaja uključuje povezivanje sa računarom ili POS terminalom putem USB kabla ili serijskog porta, ali također mora biti povezan i sa izvorom napajanja.

Slika 37 - External Powered set kablova za povezivanje čitača kartica sa POS Terminalom

Ovaj tip uređaja se često koristi kada čitač zahtijeva više energije za obradu podataka ili kada se koristi u okruženju sa velikim brojem transakcija. Nakon povezivanja, čitač treba da bude prepoznat od strane sistema.



Slika 38 - Čitač kartica kompanije Equinox Payments koji koristi External Powered set kablova za prenos podataka i napajanje

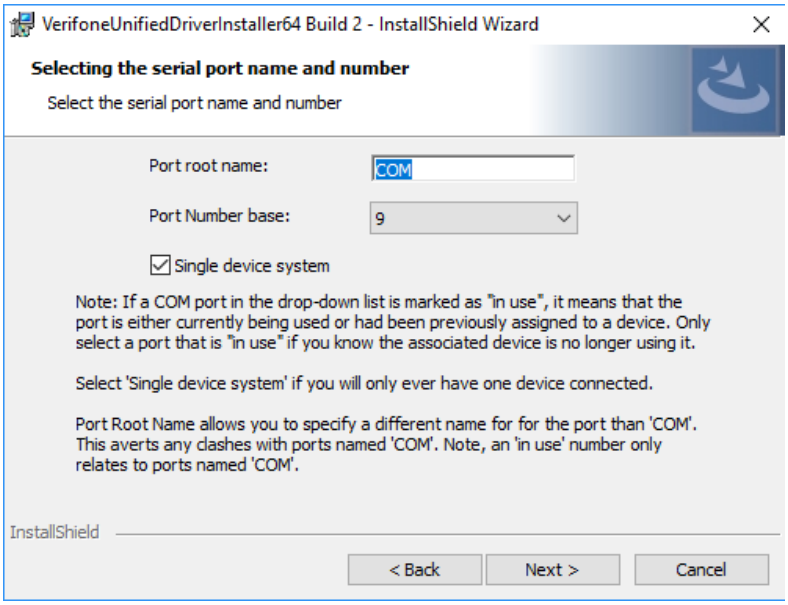
Ethernet čitači kartica omogućavaju povezivanje putem mreže, što ih čini pogodnim za veće sisteme gde je potrebno centralizovano upravljanje uređajima. Instalacija uključuje povezivanje čitača sa mrežom putem Ethernet kabla, što omogućava uređaju da komunicira sa serverom ili POS terminalom preko lokalne mreže. Ethernet čitači kartica često zahtijevaju konfiguraciju IP

adrese i mogu koristiti protokole poput TCP/IP za komunikaciju sa serverima za autorizaciju transakcija. Moguće je da čitač neće raditi odmah, pa je potrebno provjeriti mrežnu konfiguraciju i pristup mreži kako bi se osigurao nesmetan rad uređaja.

Instalacija **bežičnog** čitača kartica koji koristi Wi-Fi obuhvata povezivanje uređaja sa lokalnom bežičnom mrežom. Prvo, potrebno je osigurati da uređaj bude u dometu Wi-Fi signala, a zatim ga povezati na mrežu putem odgovarajuće aplikacije ili softverskog interfejsa. Tokom ovog procesa, korisnik unosi naziv mreže (SSID) i šifru, čime omogućava uređaju da se poveže sa internetom ili lokalnom mrežom. Nakon povezivanja na mrežu, čitač kartica treba da bude prepoznat u POS sistemu i može se koristiti za obradu transakcija.

Slika 39 - Bežični čitač kartica kompanije Equinox Payments

Drajveri su potrebni za omogućavanje komunikacije između uređaja i operativnog sistema. Bez odgovarajućih drajvera, uređaj neće funkcionisati ispravno. Instalacija drajvera obično uključuje preuzimanje odgovarajuće verzije sa zvanične web stranice proizvođača ili sa diska koji dolazi uz uređaj. Nakon preuzimanja, korisnik pokreće instalacijski program i prati uputstva.

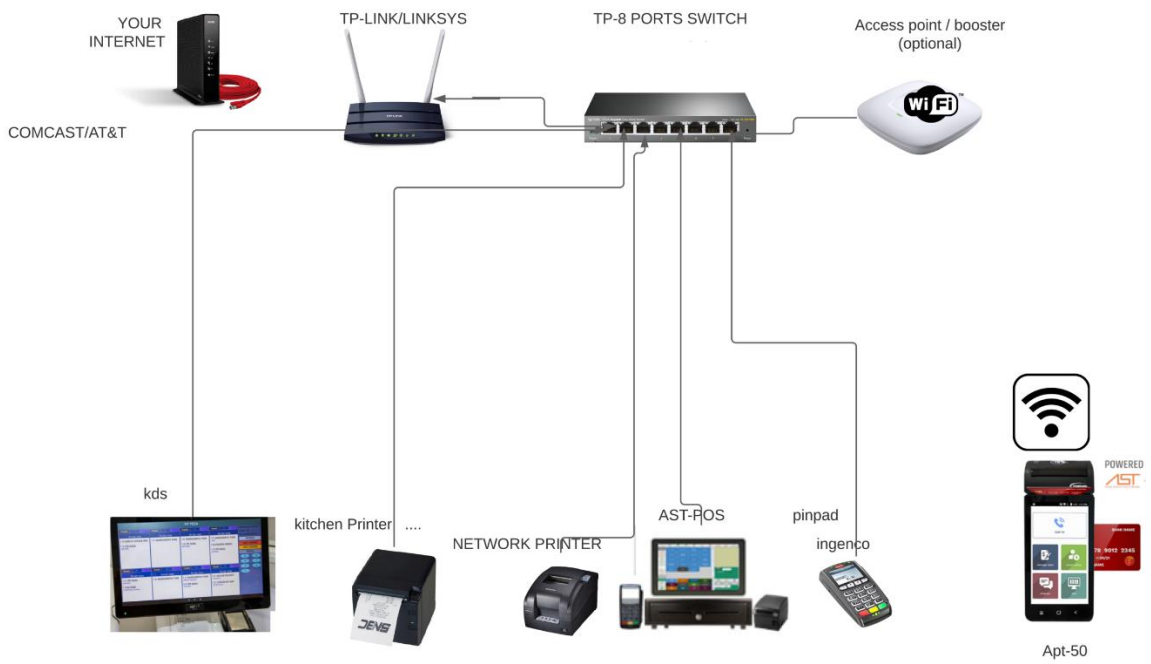


Slika 40 - Primjer instalacije Verifone USB drajvera

Firmver (engl. Firmware) je softver koji se nalazi direktno u uređaju i omogućava njegov rad. Ažuriranje firmvera može poboljšati performanse uređaja, dodati nove funkcije, kao i ispraviti greške u prethodnim verzijama. Da bi se ažurirao firmver, korisnik mora preuzeti najnoviju verziju sa zvanične stranice proizvođača uređaja. Ažuriranje obično uključuje povezivanje uređaja sa računarom putem USB, Ethernet ili bežične veze, a zatim pokretanje softverskog alata koji omogućava instalaciju nove verzije firmvera. Postupak može biti automatski ili zahtijeva unos komandi, u zavisnosti od proizvođača uređaja. Tokom ovog procesa, važno je pratiti uputstva, jer prekid u ažuriranju može dovesti do oštećenja firmvera i neispravnog rada uređaja.

4.1.3. Mrežni uređaji

Prekidač (engl. Switch) je mrežni uređaj koji povezuje različite uređaje unutar lokalne mreže (LAN) i omogućava im da međusobno komuniciraju. On usmjerava mrežni saobraćaj između uređaja u mreži, koristeći MAC adrese za prepoznavanje i usmjeravanje podataka na pravu destinaciju. U restoranima, switch-evima se obično povezuju POS terminali, čitači kartica, računari i drugi uređaji u mreži, omogućujući brzu i efikasnu razmjenu podataka. Dobro konfigurisani switch-evima omogućavaju segmentaciju mreže (npr. odvajanje POS sistema od internetske mreže), što poboljšava sigurnost i performanse



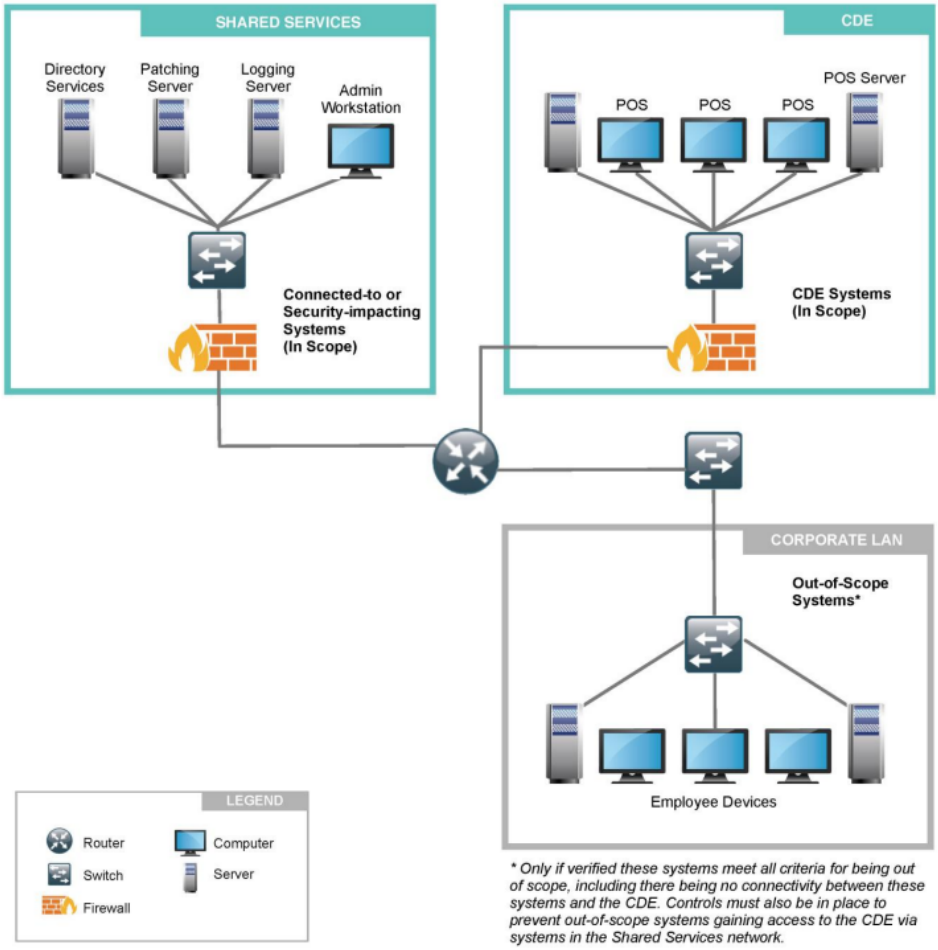
Slika 41 - Konfiguracija Switch-a unutar restorana

Firewall je uređaj koji filtrira mrežni saobraćaj između različitih mrežnih segmenata, obično između interne mreže (kao što je LAN) i spoljnog svijeta (interneta). Njegova glavna funkcija je blokiranje neovlaštenog pristupa i zaštita od različitih vrsta napada.

U restoranskim i ugostiteljskim okruženjima, firewall štiti kritične podatke poput informacija o karticama kupaca, transakcijama i poslovnim podacima.

Slika 42 - Firewall uređaj kompanije WatchGuard

Firewall se konfiguriše da dozvoli samo specifične vrste saobraćaja, čime se smanjuje rizik od napada, kao što su DDoS napadi ili pokušaji hakovanja.



Slika 43 - Segmentacija mreže i upotreba Firewall-a

4.2. Ažuriranje softvera

Ažuriranje softvera je ključan korak u očuvanju sigurnosti, funkcionalnosti i usklađenosti sa standardima kao što je PCI DSS (engl. Payment Card Industry Data Security Standard). Softverske zakrpe koje dolaze s ažuriranjima često rješavaju otkrivene sigurnosne ranjivosti, čime se smanjuje rizik od potencijalnih napada ili zloupotreba.

Pored sigurnosnih aspekata, ažuriranja često donose nove funkcionalnosti i optimizaciju postojećih sistema, čime se omogućava bolje korisničko iskustvo i efikasniji rad sistema. Uvođenjem najnovijih verzija, organizacije osiguravaju usklađenost sa aktuelnim tehničkim i pravnim zahtjevima industrije.

Neadekvatna primjena ažuriranja može dovesti do povećane izloženosti sigurnosnim prijetnjama, gubitka podataka ili čak nepoštovanja regulativa, što može rezultirati ozbiljnim pravnim posljedicama ili gubitkom povjerenja klijenata.

4.2.1. Ažuriranje Windows operativnog sistema

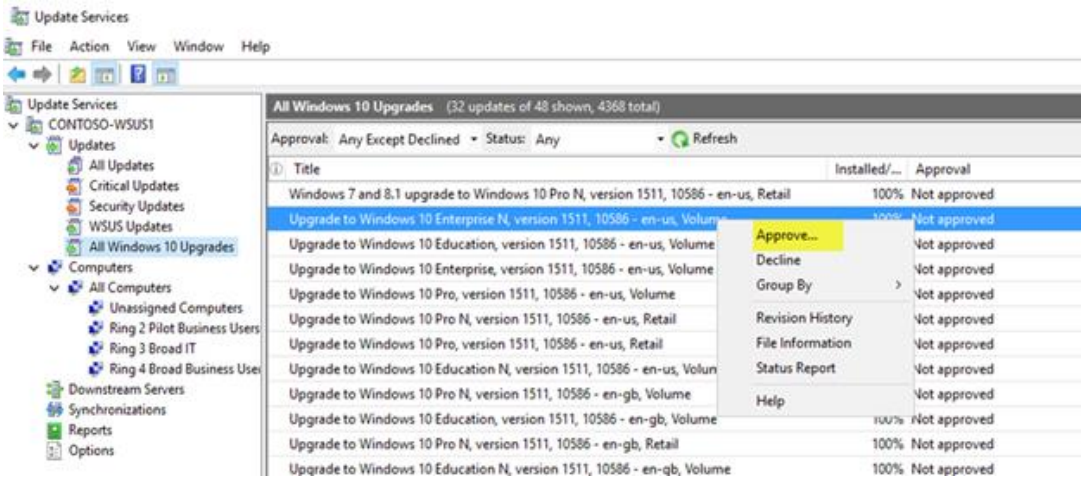
Ažuriranje Windows operativnog sistema je važno za sigurnost i stabilnost POS terminala i prateće infrastrukture u sistemima za plaćanje. Windows OS se često koristi na back-office serverima, radnim stanicama i naprednim POS uređajima, što ga čini osnovom za pouzdan rad ovih sistema. Microsoft redovno objavljuje sigurnosne zakrpe (engl. patch) koje adresiraju poznate ranjivosti, čime se spriječavaju malveri, ransomware napadi i neovlašteni pristupi.

Slika 44 - Opcija u postavkama Windows OS za mogućnost instalacije ili za provjeru ako su novije verzije dostupne

Osim sigurnosnih aspekata, redovno ažuriranja operativnog sistema osigurava usklađenost sa standardima poput PCI DSS. Ova usklađenost uključuje aktuelne protokole enkripcije, kao što su TLS 1.2 ili 1.3, što je ključno za sigurnu komunikaciju u platnim sistemima. Ažuriranja poboljšavaju performanse sistema i stabilnost aplikacija, omogućavajući kompatibilnost sa novim hardverom i softverom.

Korištenje alata poput Windows Server Update Services (WSUS) omogućava centralizovano upravljanje ažuriranjima, čime se smanjuju prekidi u radu. Planiranje ažuriranja tokom vanrednih

sati, testiranje prije implementacije u produkciji i pravljenje sigurnosnih kopija dodatno smanjuju rizik. Kod sistema za plaćanje, gdje su prekidi u radu kritični, ovakva praksa je neophodna.

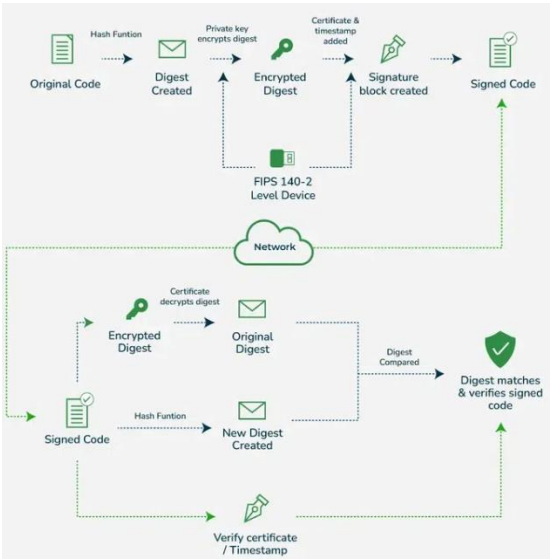


Slika 45 - Grafički interfejs Windows Server Update Services za centralizovano ažuriranje

Ukoliko POS terminal koristi Windows Embedded, ažuriranja mogu obezbjediti kompatibilnost sa novim verzijama aplikacija za plaćanje ili protokola za enkripciju, što smanjuje rizik od kvarova i nekompatibilnosti.

4.2.2. Sigurnosni sertifikati (engl. certificates) i enkripcija

Sigurnosni sertifikati i enkripcija ključni su za očuvanje povjerljivosti i integriteta komunikacije u sistemima za plaćanje, posebno kod POS terminala i prateće infrastrukture. Digitalni sertifikati se koriste za autentifikaciju i uspostavljanje šifrovanih veza između terminala, servera i drugih komponenti sistema. Redovno obnavljanje ovih sertifikata neophodno je kako bi se izbjegli prekidi u radu sistema i osigurala zaštita od potencijalnih napada.



Slika 46 - Digitalni setifikat

Usklađenost sa standardima kao što je TLS (engl. Transport Layer Security) osigurava da se koriste najnoviji protokoli enkripcije, koji su otporniji na moderne oblike cyber prijetnji. Neadekvatno upravljanje sertifikatima može dovesti do ozbiljnih posljedica, kao što su kompromitovanje povjerljivih podataka ili prekid usluge. Preporučuje automatsko praćenje datuma isteka sertifikata i implementacija procedura za njihovu pravovremenu obnovu. Korištenje sertificiranih rješenja i usklađenost sa industrijskim standardima, kao što su PCI DSS i P2PE, obezbjeđuju viši nivo sigurnosti i povjerenja korisnika.

4.3. Monitorisanje (engl. Monitoring) sistema

Monitoring sistema je ključan za obezbjeđivanje kontinuiteta rada, optimizaciju performansi i brzo otkrivanje problema u IT okruženju, posebno kod kritičnih sistema poput POS terminala i sistema za plaćanje. Alati za monitoring, poput Splunk-a, omogućavaju praćenje svih ključnih aspekata sistema u realnom vremenu, što uključuje performanse, sigurnosne incidente i operativne greške.

Slika 47 - Logo Splunk-a

Jedna od osnovnih prednosti monitoringa je identifikacija grešaka u realnom vremenu, što omogućava brzo reagovanje na probleme prije nego što eskaliraju u ozbiljnije kvarove ili gubitke. Na primjer, otkrivanje povećanog broja grešaka u transakcijama može ukazivati na problem sa komunikacijom između POS terminala i servera, što se može brzo otkloniti uz pravovremenu analizu logova.

Splunk se može koristiti na primjere kao što su pronalazak grešaka za određenu kompaniju u posljednjih sedam dana:

```
index=your_index_name sourcetype=your_sourcetype_name CompanyID="12345" error
earliest=-7d@d latest=now
| stats count by error_message
| sort -count
```

Ovaj query pretražuje indeks i sourcetype gdje se pojavljuju logovi za određeni CompanyID (12345) i filtrira zapise koji sadrže riječ "error". Rezultati prikazuju broj pojavljivanja svake greške u poslednjih sedam dana, sortirane po učestalosti.

U sistemima kao što su sigurnosno plaćanje, može se koristiti query koji će izračunati prosječno trajanje transakcija (engl. lapsed time):

```
index=your_index_name sourcetype=your_sourcetype_name
transaction_status="completed"
| eval transaction_time=strptime(transaction_end_time, "%Y-%m-%d %H:%M:%S") -
strptime(transaction_start_time, "%Y-%m-%d %H:%M:%S")
| stats avg(transaction_time) as avg_lapsed_time, max(transaction_time) as
max_lapsed_time, min(transaction_time) as min_lapsed_time
```

Ovaj query računa prosječno, maksimalno i minimalno trajanje transakcija označenih kao "completed". Pretpostavlja da logovi sadrže vremenske oznake za početak (transaction_start_time) i kraj (transaction_end_time) transakcije u formatu "%Y-%m-%d %H:%M:%S".

5. Podrška korisnicima i rješavanje problema

Struktura podrške u IT industriji, posebno u sistemima za plaćanje, zasniva se na višeslojnom modelu kako bi se efikasno rešavali problemi, optimizovao rad sistema i osigurala vrhunska korisnička podrška. Svaki nivo podrške ima specifične odgovornosti i veštine, omogućavajući podelu zadataka i rešavanje problema na najprikladniji način.

5.1. Level-1 podrška (prvi nivo)

L1 je prva tačka kontakta za korisnike i fokusira se na osnovno rješavanje problema i eskalaciju prema višim nivoima kada je potrebno. Na primer, kao L1 agenat, osnovne odgovornosti uključuju pružanje podrške korisnicima iz različitih sektora za objašnjenje osnovnih funkcija sistema za plaćanje i rješavanje osnovnih problema. L1 agenti često asistiraju pri evidentiranju grešaka u transakcijama i pomažu u rješavanju pitanja kao što su neuspijele transakcije ili refundacije, uz minimalno tehničko znanje. Također, pružaju osnovnu hardversku podršku, kao što je ponovno pokretanje čitača kartica, POS terminala ili provjeravanje kablova.

Slika 48 - Slikovni prikaz tehničke podrške u praksi

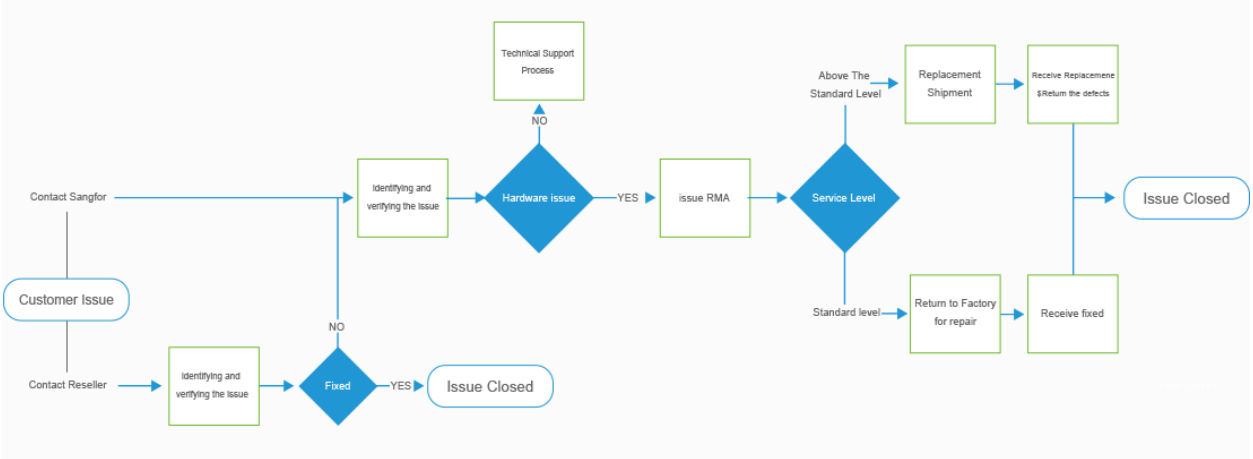
5.2. Level-2 podrška (drugi nivo)

Level 2 podrška preuzima kompleksnije zadatke koji zahtijevaju tehničko znanje i iskustvo. Ovaj nivo analizira tehničke logove, poput XML fajlova, kako bi identifikovao uzrok grešaka u transakcijama i pružio rješenja.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Created from PDF via Acrobat SaveAsXML -->
<!-- Mapping Table version: 28-February-2003 -->
- <TaggedPDF-doc>
    <?xpacket begin='' id='W5M0MpCehiHzreSzNTczkc9d'?>
    <?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
  - <x:xmpmeta x:xmptk="Adobe XMP Core 5.2-c001 63.139439, 2010/09/27-13:37:26 " xmlns:x="adobe:ns:meta/">
    - <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
      - <rdf:Description xmlns:xmp="http://ns.adobe.com/xap/1.0/" rdf:about="">
          <xmp:CreateDate>2011-04-06T17:22:05Z</xmp:CreateDate>
          <xmp:CreatorTool>ESRI ArcSOC 9.2.0.1324</xmp:CreatorTool>
          <xmp:ModifyDate>2011-04-07T08:17:15-06:00</xmp:ModifyDate>
          <xmp:MetadataDate>2011-04-07T08:17:15-06:00</xmp:MetadataDate>
        </rdf:Description>
      - <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">
          <xmpMM:DocumentID>uuid:323e04f1-1033-4485-be82-e60a7573f2ec</xmpMM:DocumentID>
          <xmpMM:InstanceID>uuid:6329c275-adcd-4082-bf5a-708d7846e55c</xmpMM:InstanceID>
        </rdf:Description>
      - <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/">
          <dc:format>xml</dc:format>
        </rdf:Description>
      </rdf:RDF>
    </x:xmpmeta>
    <?xpacket end="w"?>
    <?xpacket end='r'?>
  - <Figure>
      <ImageData src="images/WA_Dayton_20110406_TM_geo_img_0.jpg"/>
    </Figure>
</TaggedPDF-doc>
```

Slika 49 - Primjer XML (eXtensible Markup Language) fajla

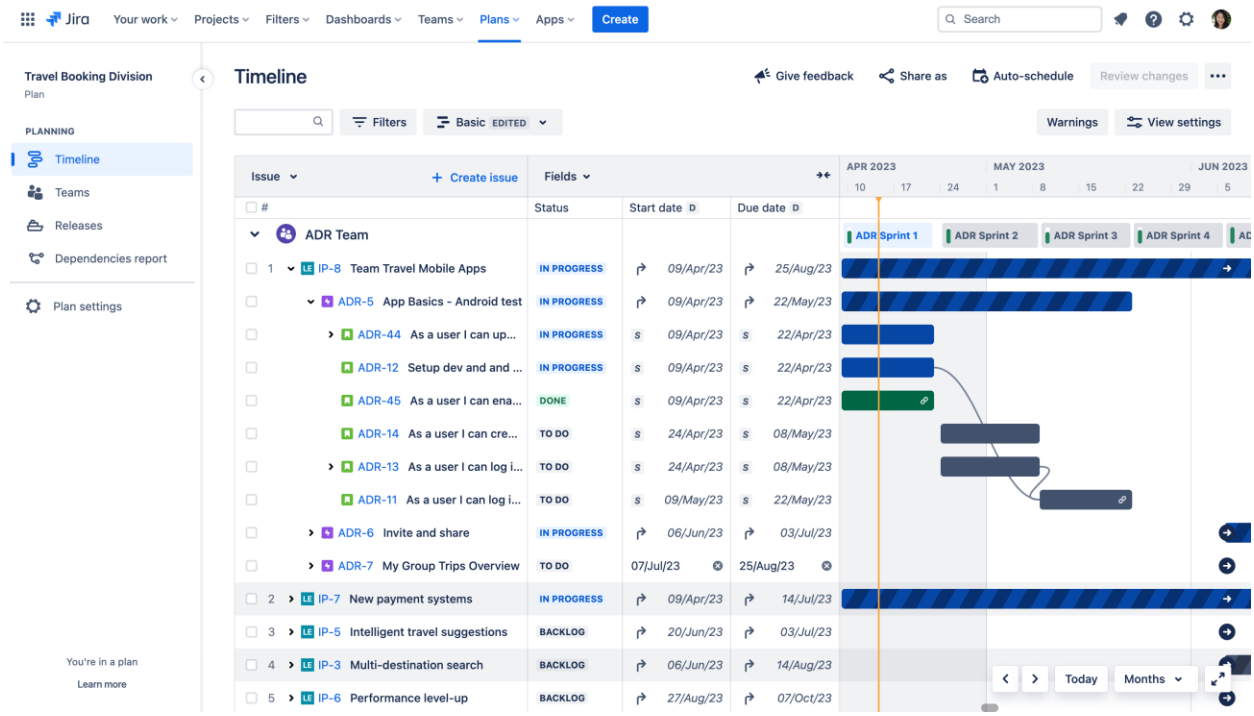
Kao Level 2 agent, uloga uključuje rad sa procesorima plaćanja, tokenima visokih vrijednosti i Merchant ID-ovima, kao i rješavanje problema koji se odnose na elektronsku trgovinu i fizičke prodavnice. Pored toga, Level 2 se često bavi hardverskim problemima na dubljem nivou, poput identifikovanja kvarova na čitačima kartica (Equinox, VeriFone) i organizovanja njihove zamjene.



Slika 50 - Dijagram procesa zamjene hardvera

5.3. Level-3 podrška (treći nivo)

Level 3 podrška je odgovorna za rješavanje najsloženijih problema i obezbjeđivanje trajnih rješenja. Ovaj nivo uključuje dubinsku analizu grešaka koristeći napredne alate poput Splunk-a za pretragu logova, kao i saradnju sa timovima za razvoj (L4) radi popravke softverskih bagova.



Slika 51 - JIRA slučajevi za otklanjanje prijavljenih grešaka

Kao Level 3 agent, fokus je na rješavanju problema koji prelaze opseg L1 i L2 podrške, kreiranju vodiča za rješavanje problema i treniranju agenata nižih nivoa. Level 3 također aktivno doprinosi analizi sigurnosnih incidenata i optimizaciji sistema i vođenju ključnih projekata, poput implementacije novih funkcionalnosti ili unapređenja performansi sistema.

5.4. Primjeri čestih problema

Greške u transakcijama često uključuju neuspješna plaćanja ili progrešno procesuirane iznose. Ovo može biti posljedica komunikacionih problema, progrešnih podešavanja ili softverskih grešaka. Ovi problemi se najčešće rješavaju na slijedeće načine:

- *Analiza logova* - Koristiti alate kao što su Splunk ili slični za pretragu logova transakcija (XML logovi, debouti). Identifikovati specifične greške, poput "timeout" ili "invalid token" errora;
- *Validacija podešavanja* - Provjeriti ispravnost Merchant ID-a, tokena i procesorskih postavki u backend-u;

- *Ponovno procesuiranje* - Ako se radi o privremenom problemu, pokušati ponovo obraditi transakciju ili izvršiti refundaciju ako je neophodno;
- *Eskalacija* - Za greške koje se ne mogu rješiti, prosljediti problem na L3 nivo radi dublje analize ili na razvojni tim ako je potrebna softverska intervencija;

Kvarovi hardvera česti problemi i uključuju nefunkcionalne čitače kartica, probleme sa POS terminalima ili printerima.

Slika 52 - Hardverski oštećeni čitači kartica kompanije Ingenico

Osnovni postupci u rješavanju hardverskih problema kod čitača kartica:

- *Osnovno rješavanje problema* - Provjeriti napajanje uređaja, kablove i povezanost sa mrežom;
- *Ponovno pokretanje* - Resetartovati uređaj ili POS terminal;
- *Firmware update* - Provjeriti da li uređaj ima najnoviji firmware i ažurirati ako je potrebno;
- *Zamjena hardvera* - Ako problem nije rješiv, organizovati RMA (engl. Return Merchandise Authorization) i poslati zamjenski uređaj;
- *Proaktivno praćenje* - Koristiti monitoring alate za prepoznavanje znakova potencijalnih kvarova, kao što su prekidi u komunikaciji sa uređajem;

Problemi sa **mrežnom povezanošću** mogu ometati komunikaciju između POS terminala i servera, što dovodi do prekida u radu ili kašnjenja u obradi transakcija.

Neki od osnovnu postupaka koje treba potupiti u slučaju mrežnih problema:

- *Dijagnostika mreže* - Koristiti mrežne alate (ping, traceroute) za provjeru konektivnosti između terminala i servera;
- *Ispravka konfiguracije* - Provjeriti IP adresu, DNS podešavanja i firewall pravila;
- *Preusmjeravanje* - Ako primarna mreža ne funkcioniše, preusmjeriti POS terminal na rezervnu mrežu ako postoji;
- *Saradnja sa mrežnim timom* - Ako problem prevazilazi lokalne mogućnosti, uključiti mrežni tim za rješavanje problema na višem nivou;

5.5. Dokumentacija za korisnike

Dokumentacija treba da bude jednostavna, jasna i lako dostupna korisnicima, bilo u štampanoj ili online formi. Osnovne komponente uključuju korisničke priručnike koji objašnjavaju kako koristiti POS sisteme, najčešće postavljana pitanja (engl. FAQ – Frequently Asked Questions) koja pomažu korisnicima da brzo rješe uobičajene probleme, kao i kontakt informacije za tehničku podršku. Korištenje vodiča sa screenshot-ovima i video tutorijala može dodatno pomoći korisnicima da brzo savladaju osnovne funkcionalnosti i rješe poteškoće poput grešaka u transakcijama ili hardverskim problemima.

Vrste dokumentacije:

- Korisnički priručnici - Priručnici obuhvataju osnovne funkcionalnosti POS sistema, kao i detalje o tome kako koristiti terminale za obradu plaćanja, izdavanje računa, rad sa povratima i refundacijama i rješavanje osnovnih problema. Priručnici treba da budu jednostavni i jasni, sa screenshot-ovima i vizuelnim prikazima;

- FAQ (Često postavljana pitanja) - Dokument koji pruža odgovore na najčešća pitanja korisnika, kao što su "Šta da radim ako mi terminal ne radi?" ili "Kako da resetujem POS uređaj?";

- Tehnička podrška i kontakti - Uputstva o tome kako kontaktirati tehničku podršku, kao i informacije o tome šta treba pripremiti prije nego što se pozove podrška (npr. broj transakcije, serijski broj uređaja);

- Video tutorijali (webinar) - Korištenje video materijala može biti efikasan način da korisnici vide kako da koriste POS sistem u realnom vremenu, sa jasno objašnjenim koracima;

ZAKLJUČAK

Razvoj i implementacija savremenih sistema za plaćanje predstavlja ključnu kariku u globalnom finansijskom sistemu, omogućavajući efikasno i sigurno obavljanje transakcija. Kako se poslovanje sve više oslanja na elektronske metode plaćanja, potreba za sigurnošću i usklađenošću sa standardima poput PCI DSS postaje imperativ za sve učesnike u procesu. P2PE enkripcija i tokenizacija predstavljaju napredne sigurnosne mjere koje štite podatke korisnika, dok efikasna administracija sistema omogućava pravilno funkcionisanje i brzu reakciju na potencijalne probleme.

Implementacija i održavanje ovih sistema zahtjeva visok nivo tehničke ekspertize, kao i stalnu obuku i podršku korisnicima kako bi se obezbjedila visoka kvaliteta usluge i zaštita od prevara. Kroz ovaj rad, jasno je da bezbjednost, efikasnost i usklađenost sa industrijskim standardima čine osnovne temelje za razvoj modernih sistema za plaćanje, a njihova implementacija i podrška ostaju ključevi za njihovu dugoročnu održivost i uspijeh.

POPIS SLIKA

CITATNI IZVORI

[1] S. Riksbank, »Payment systems: Historical evolution and literature review,« 2019. [Mrežno]. Available: https://www.riksbank.se/globalassets/media/rapporter/pov/artiklar/engelska/2019/190613/er-2019_1-payment-systems--historical-evolution-and-literature-review.pdf.

[2] OriginStamp, »The evolution of digital payments: A timeline,« 2021. [Mrežno]. Available: https://originstamp.com/blog/the-evolution-of-digital-payments-a-timeline/.

[3] O. Slozko i A. Pelo, »Problems and Risks of Digital Technologies Introduction into E-Payments,« *Transformations in Business & Economics,* svez. 14, p. 42–59, 2015.

[4] Capgemini, »2020 World Payments Report: Transforming into Digital Masters in the Next Normal,« 2020. [Mrežno]. Available: https://www.sogeti.com/explore/reports/world-payments-report-2020/.

[5] R. Rajpal, »SoftwareSuggest,« [Mrežno]. Available: https://www.softwaresuggest.com/blog/point-of-sales-pos-terminal/. [Pokušaj pristupa 17 November 2024].

[6] Clover Blog, »Clover Blog,« [Mrežno]. Available: https://blog.clover.com/what-is-a-card-reader-how-does-it-work/. [Pokušaj pristupa 17 Novembar 2024].

[7] Investopedia, »Card Reader,« Investopedia, [Mrežno]. Available: https://www.investopedia.com/terms/c/card-reader.asp. [Pokušaj pristupa 17 Novembar 2024].

[8] M. Victor, »Medium,« Step-by-step guide on developing a POS terminal application, [Mrežno]. Available: https://medium.com/@victormba/step-by-step-guide-on-developing-a-pos-terminal-application-4c5fb32d50b8. [Pokušaj pristupa 17 Novembar 2024].

[9] EMVCo, »EMVCo,« Worldwide EMV Deployment Statistics, [Mrežno]. Available: https://www.emvco.com/about-us/worldwide-emv-deployment-statistics/. [Pokušaj pristupa 17 Novembar 2024].

[10] T. Anthea, »Checkout.com,« The benefits of end-to-end payment processing, 26 Januar 2023. [Mrežno]. Available: https://www.checkout.com/blog/choosing-an-end-to-end-payments-solution. [Pokušaj pristupa 17 Novembar 2024].

[11] HighRadius, »What is a payment gateway and how it works,« HighRadius Blog, [Mrežno]. Available: https://www.highradius.com/resources/Blog/what-is-a-payment-gateway-and-how-it-works/. [Pokušaj pristupa 17 Novembar 2024].

[12] Z. Bezhovski, »The Future of the Mobile Payment as Electronic Payment System,« *European Journal of Business and Management,* svez. 8, p. 2222–2839, 2016.

[13] S. Z. J. T. Isaac, »Secure Mobile Payment Systems,« *Journal of Enterprise Information Management,* svez. 22, p. 317–345, 2014.

[14] K. Subaramaniam, J. M. Garding, R. Kolandaisamy i A. B. Jalil, »The impact of E-Wallets for current generation,« *Journal of Advanced Research in Dynamical and Control Systems,* svez. 12, p. 751–759, 2020.

[15] ACI Worldwide, »Point-to-Point Encryption (P2PE),« ACI Worldwide, [Mrežno]. Available: https://www.aciworldwide.com/p2p-encryption. [Pokušaj pristupa 18 Novembar 2024].

[16] Fiserv, »P2PE and Tokenization to Lower Data Breach Impact,« [Mrežno]. Available: https://www.carat.fiserv.com/content/dam/carat/us/en/documents/pdf/P2PE_Tokenization_to_Lower_Data_Breach_Impact.pdf. [Pokušaj pristupa 18 Novembar 2024].