Analiza ekosustava mobilnog plaćanja

Gospočić, Zdravko

Sveučilište u Zagrebu
Fakultet prometnih znanosti

Zdravko Gospočić

Analiza ekosustava mobilnog plaćanja

DIPLOMSKI RAD

Zagreb, 2020.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 1. travnja 2020.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Projektiranje informacijsko komunikacijskih usluga**

DIPLOMSKI ZADATAK br. 5890

Pristupnik: **Zdravko Gospočić (0135235942)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza ekosustava mobilnog plaćanja**

Opis zadatka:

Opisati značajke sustava i usluga mobilnog plaćanja. Analizirati moguću primjenu usluga plaćanja mobilnim uređajem i ponašanje korisnika. Definirati tehnologije i aplikacije korištene za usluge mobilnog plaćanja. Istražiti sigurnosne aspekte i mogućnosti zaštite elemenata ekosustava mobilnog plaćanja. Prikazati rezultate istraživanja provedbom ankete.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA EKOSUSTAVA MOBILNOG PLAĆANJA

MOBILE PAYMENT ECOSYSTEM ANALYSIS

Mentor: dr. sc. Siniša Husnjak

Student: Zdravko Gospočić
0135235942

Zagreb, rujan 2020.

SAŽETAK

U istraživanju su objašnjeni svi elementi ekosustava mobilnog plaćanja; korisnik, terminalni uređaj, mreža, usluge i aplikacije, poslužitelji, posrednici, financijske institucije, mrežni operatori i drugi bitni sudionici koji čine vrijednosni lanac u ostvarivanju usluga mobilnog plaćanja. Provođenjem ankete i analizom ponašanja korisnika obrazložena je problematika mobilnog plaćanja u današnjem načinu života. Nabrojani su razni novi načini i tehnologije u procesu mobilnog plaćanja. Također su nabrojani svi mehanizme zaštite osobnih podataka i financijskih sredstava korisnika koji koriste usluge mobilnog plaćanja te tako obrazloženi sigurnost i moguće prijetnje kako bi svatko mogao iz ovoga rada zaključiti koliko je mobilno plaćanje sigurno. Prema rezultatima dobivenim istraživanjem provedbom ankete može se zaključiti da su usluge mobilnog plaćanja popularnija kod mlađe populacije korisnika, te da kao zadovoljstvo korištenja ovakvog načina plaćanja korisnici najviše ističu brzinu obavljanja svih potrebnih poslova.

KLJUČNE RIJEČI: ekosustav; vrijednosni lanac; Near Field Communication (NFC); mobilno plaćanje; mobilno bankarstvo; aplikacije mobilnog plaćanja

SUMMARY

The research explains all the elements of the mobile payment ecosystem; user, terminal device, network, services and applications, servers, intermediaries, financial institutions, network operators and other important participants that form the value chain in the realization of mobile payment services. By conducting a survey and analyzing the behavior of users, the problem of mobile payments in today's way of life is explained. Various new ways and technologies in the process of mobile payment are listed. Also listed are all the mechanisms for the protection of personal data and financial resources of users who use mobile payment services, and thus explained the security and possible threats so that everyone can conclude from this paper how secure mobile payment is. According to the results of the survey, it can be concluded that mobile payment services are more popular with the younger population of users, and that as a pleasure to use this method of payment, users emphasize the speed of all necessary tasks related to payment.

KEYWORDS: ecosystem; value chain; Near Field Communication (NFC); mobile payments; mobile banking; mobile payment applications

Sadržaj:

1. UVOD....1
2. OPĆENITO O SUSTAVU I USLUGAMA MOBILNOG PLAĆANJA....2
2.1. Razvoj mobilnog plaćanja....2
2.2. Princip rada beskontaktnog plaćanja....4
2.3. Mobilni novčanik....5
2.3.1. Tipovi mobilnih novčanika....5
2.3.2. Zaštita mobilnog novčanika....6
2.3.3. Važni dionici mobilnog novčanika....8
3. NAČINI PLAĆANJA MOBILNIM UREĐAJEM....10
3.1. SMS plaćanja....10
3.2. Plaćanje korištenjem WEB servisa....12
3.4. Isplate temeljene na zvučnim valovima....15
3.5. Plaćanja magnetskim sigurnim prijenosom (MST)....17
3.6. Plaćanje QR kodom....18
3.7. Plaćanje NFC tehnologijom....19
3.7.1. Vrste NFC komunikacije....19
3.7.2. Sigurnost plaćanja NFC tehnologijom....22
3.8. HCE Tehnologija....23
4. ANALIZA EKOSUSTAVA MOBILNOG PLAĆANJA....26
4.1. Lanac vrijednosti ICT ekosustava....26
4.1.1. Korisnik....27
4.1.2. Korisnički terminalni uređaji....28
4.1.3. Mreža....30
4.1.4. Poslužitelj....31
4.1.5. Usluge i aplikacije....32
4.1.6. Sadržaj....38
4.2. Sudionici poslovnog modela ekosustava mobilnog plaćanja....39
4.2.1. Operatori mobilne mreže....41
4.2.2. Financijske institucije (banke)....43
4.2.3. Agregatori....44

4.2.4. Trgovci 45
4.2.5. Platne mreže 46
4.2.6. Korisnici 47
5. SIGURNOST I ZAŠTITA USLUGA MOBILNOG PLAĆANJA 49
5.1. Prijetnje i napadi na ekosustav mobilnog plaćanja 50
5.2. Metode zaštite i ranjivosti ekosustava mobilnog plaćanja 53
6. REZULTATI ISTRAŽIVANJA PROVEDBOM ANKETE 57
7. ZAKLJUČAK 68
LITERATURA 69
POPIS KRATICA 71
POPIS SLIKA 74
POPIS GRAFIKONA 75
POPIS TABLICA 75

1. UVOD

Mobilni uređaji te njihove funkcije i usluge koje nude postali su nezamjenjivi dio života. Danas nema više toliko razlike da samo mlađa populacija koristi mobilni uređaj, nego se dobar dio ljudi srednjih godina pa čak i starije životne dobi odlučio koristiti mobilne uređaje u razne svrhe, jer su shvatili da je to način na koji svijet danas funkcionira te da će bez korištenja mobilnog uređaja neće biti u skladu s vremenom u kojem žive. S obzirom na to da više dobnih skupina koristi mobilne uređaje kao rezultat toga se i povećava opseg tržišta mobilnog plaćanja te korištenja mobilnog uređaja kao jednog od modernijih načina plaćanja koji predstavljaju budućnost. U ovom radu će se istražiti cijeli ekosustav mobilnog plaćanja kroz sve sudionike vrijednosnog lanca, kao i različiti načini mobilnog plaćanja.

Osnovni predmet promatranja ovoga rada jest ekosustav mobilnog plaćanja uz istraživanje različitih načina, tehnologija i aplikacija korištenih za ostvarivanje kvalitetnog rada i funkcioniranja cijelog ekosustava mobilnog plaćanja. Tako će se kroz niz grafova i arhitektura objasniti kako izgleda proces mobilnog plaćanja od pošiljatelja do primatelja. Bit će objašnjen svaki sudionik pojedinačno te zašto je on bitan dio ekosustava mobilnog plaćanja te kako ostvaruje svoje prihode i koja mu je svrha egzistencije u ekosustavu mobilnog plaćanja. Na temelju navedenog će budući korisnici mobilnog plaćanja imati uvid kroz što sve mora proći njihova novčana transakcija kada koriste usluge mobilnog plaćanja. Krajnji rezultat provedbom ankete bit će doći do zaključka koliko je ispitana skupina upoznata s ekosustavom mobilnog plaćanja te koriste li neki od načina mobilnih plaćanja i koliko te sustave smatraju korisnim i sigurnim ili i dalje vjeruju tradicionalnom gotovinskom i kartičnom plaćanju.

Cilj istraživanja jest pokazati kako bi mobilno plaćanje pomoglo cijeloj populaciji te pojednostavilo način života i ubrzalo proces plaćanja proizvoda, robe i usluga te kako je cijeli ekosustav mobilnog plaćanja siguran i ima svoje načine zaštite svih korisnikovih podataka. Uz načine plaćanja nabrojat će se 3 najkorištenije aplikacije mobilnog plaćanja koji su u funkciji mobilnog novčanika, a to su Samsung Pay, Google Pay te Apple Pay. Kroz njihovu arhitekturu i ekosustav detaljnije će se objasniti što se događa u pozadini kada korisnik koristi neku od aplikacija za mobilno plaćanje.

2. OPĆENITO O SUSTAVU I USLUGAMA MOBILNOG PLAĆANJA

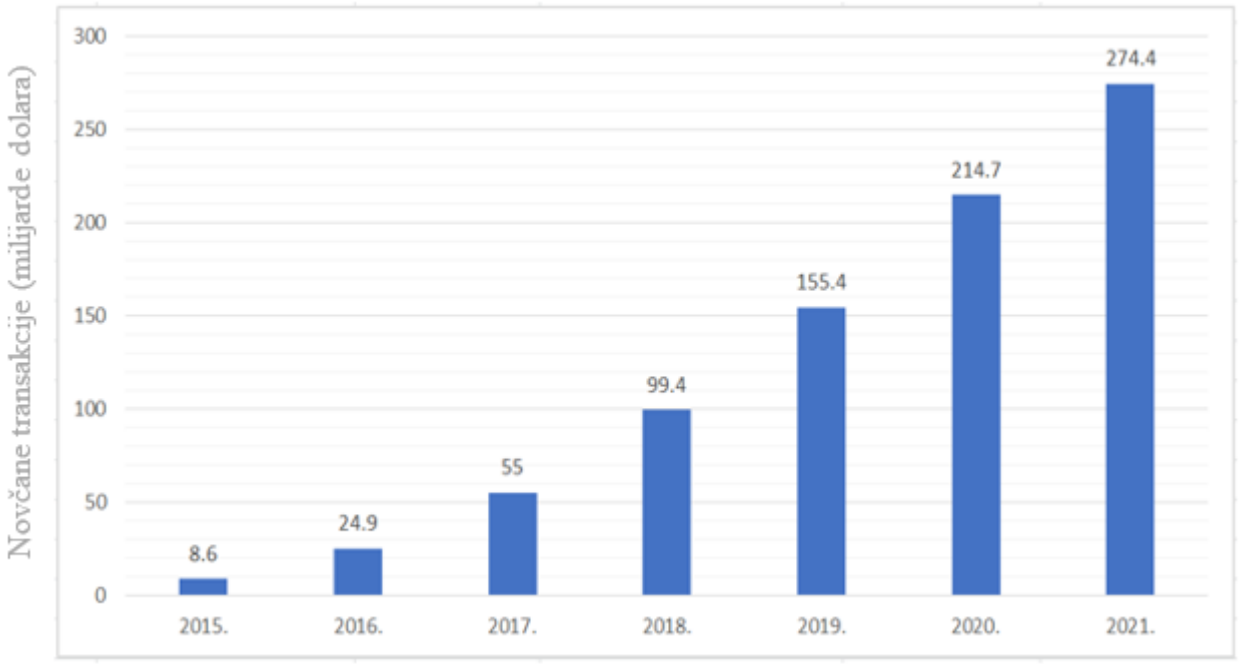
Mobilna tehnologija u najširem smislu podrazumijeva elektroničke uređaje informatičke ili komunikacijske namjene koji se mogu koristiti u pokretu, te se nazivaju mobilnim uređajima ili jednostavnije mobitelima. Također obuhvaća infrastrukturu ožičenu ili bežičnu, koja je potrebna za povezivanje i umrežavanje mobilnih uređaja s drugim stolnim ili mobilnim sustavima i uređajima. Mobilni uređaji se dijele na: mobilne komunikatore to su mobiteli i pametni telefoni, zatim na mobilna računala kao što je PDA (eng. *Personal Digital Assistant*) i na kraju na prijenosna računala ili prijenosnike (laptop, tablet, notebook). Danas su najkorišteniji mobilni uređaji jer gotovo svaka osoba ima novi Android ili Apple uređaj te ga koristi svakodnevno, razvojem aplikacija pogotovo bankarskih došlo je do olakšavanja poslovanja i platežnog procesa.

Mobilno plaćanje je novi alternativni način plaćanja. Za razliku od plaćanja u gotovini, kreditnim karticama ili čekom, korisnicima je omogućeno da plaćaju razne usluge koristeći vlastiti mobilni uređaj. Kao naprimjer naplata prijevoza, parkinga, on-line igara, računa i drugih oblika online plaćanja. Sustavi e-plaćanja ostvaruju mogućnost plaćanja dobara ili usluga preko Interneta. Kupac šalje prodavatelju podatke relevantne sa strane Interneta, a nije potrebno imati vanjsku interakciju poput računa ili potvrde preko e-pošte. Do danas je razvijen veliki broj različitih sustava elektroničkih i mobilnih plaćanja. Neki pružatelji usluga omogućuju da se kreditna kartica poveže sa SIM (*Subscriber Identity Module*) karticom korisnikova mobilnog telefona. Postoji i usluga mobilnih mikro plaćanja kao i vrijednosne kartice za plaćanje digitalnih sadržaja poput aplikacije za mobilni telefon. Mobilna plaćanja (koja obuhvaćaju mobilne novčanike i mobilne novčane prijenose) su regulirane transakcije koje se odvijaju putem mobilnog uređaja. Umjesto da se stvari plaćaju gotovinom, čekovima ili fizičkim kreditnim karticama, tehnologija mobilnog plaćanja omogućava da se to učini digitalno. Može se birati između raznih vrsta, aplikacija i načina mobilnog plaćanja koji će biti navedene kroz rad.

2.1. Razvoj mobilnog plaćanja

Tržište mobilnih plaćanja procijenjeno je na 1139,43 milijardi dolara u 2019. godini, a očekuje se da će dostići vrijednost od 4690,65 milijardi dolara do 2025. godine. Trgovine i usluge širom svijeta brzo prihvaćaju i integriraju mobilne aplikacije za plaćanje, poput Pay Pal-a, Samsung Pay-a, Apple Pay-a, Google Pay-a i drugih,. Zbog promjene načina života,

svakodnevne trgovine i naglog rasta mrežne trgovine na malo očekuje se da će se taj trend nastaviti i sljedećih mnogo godina. Uz brzo rastuću globalnu ekonomiju (Slika 1) mobilni telefoni (posebno pametni telefoni) postali su osnovna roba za pojedinca. Slično tome internet je također postao dio života mnogih ljudi pogotovo mlađe populacije. To je povećalo penetraciju pametnih telefona i korisnika interneta u cijelom svijetu, vodeći rast tržišta mobilnog plaćanja. Tvrtke mnogo ulažu u tehnologiju mobilnog plaćanja zbog značajnog rasta u industriji. Mnoge vlade također potiču banke na izgradnju infrastrukture koja će omogućiti sigurna mobilna plaćanja u ruralnim područjima, što je velika prilika za cijeli ekosustav mobilnog plaćanja i sve njegove sudionike, [6].



Slika 1: Prikaz naglog porasta broja mobilnih transakcija u milijardama dolara

Izvor: [6]

Rast potražnje za laganom i bezbrižnom kupnjom roba i usluga rezultira povećanom sklonošću potrošača prema digitalnim i bezgotovinskim plaćanjima. Glavni svjetski proizvođači, poput Apple-a i Samsung-a, osmislili su nove strategije kako bi proširili svoj domet i stekli veći udio na globalnom tržištu mobilnih plaćanja. Na grafikonu se vidi nagli porast broja mobilnih transakcija u milijardama u zadnjih 5 godina te predviđanje za 2021. godinu.

2.2. Princip rada beskontaktnog plaćanja

Da bi se razumjelo kako beskontaktno plaćanje funkcionira navest će se primjer. Ako korisnik posjeduje Samsung uređaj koji mu omogućuje da koristi opcije i usluge Samsung Paya. Podatke o kreditnoj kartici unosi na svoj mobilni uređaj gdje ih pohranjujete za kasniju upotrebu. Kasnije kupuje u trgovini koja u registru ima čitače mobilnih plaćanja. Umjesto da koristi novčanik korisnik može koristiti mobilni uređaj tako da ga prisloni nekoliko centimetara od terminala na prodajnom mjestu POS (eng. *Point of Sale*). Ovaj uređaj automatski čita podatke o plaćanju pohranjene na pametnom čipu ugrađenom u karticu, a zatim obrađuje transakciju. Svaki čip povezuje se s antenom, a POS terminali emitiraju visokofrekventni radio val koristeći NFC (eng. *Near Field Communication*) tehnologiju koji olakšava komunikaciju između čitača i telefona (slika 2). Kad je mobilni uređaj u dometu, protokol bežične komunikacije povezuje terminal i telefon, koji razmjenjuju informacije i obavljaju sigurnu transakciju, [1].

Slika 2: Prikaz beskontaktnog plaćanja na POS uređaju putem mobilnog uređaja

Izvor: [1]

2.3. Mobilni novčanik

Mobilni novčanik u osnovi je digitalni novčanik na telefonu. U aplikaciji za mobilni novčanik može se sigurno dodati i pohraniti bankovne podatke povezane s debitnom ili kreditnom karticom (neke aplikacije mobilnog novčanika omogućuju dodavanje više od jedne kartice). Umjesto da se pomoću fizičke kartice nešto plati, korisniku je omogućeno da to obavi pomoću mobilnog uređaja. Mobilni novčanik je aplikacija koja se može instalirati na pametni telefon ili je postojeća ugrađena značajka pametnog telefona. Mobilni novčanik pohranjuje podatke o kreditnoj kartici, debitnoj kartici, kuponima ili nagradnim karticama. Nakon što je aplikacija instalirana i korisnik unese podatke o plaćanju, novčanik pohranjuje podatke povezujući osobni identifikacijski format poput broja ili ključa, QR koda ili slike vlasnika sa svakom pohranjenom karticom.

Kad korisnik izvrši plaćanje trgovcu mobilna aplikacija koristi NFC tehnologiju koja koristi radio frekvencije za komunikaciju između uređaja. NFC koristi osobni identifikacijski format kreiran za korisnika za slanje podataka o plaćanju na POS-ov terminal trgovca. Prijenos informacija se obično pokreće kada korisnik maše ili drži mobilni uređaj s omogućenom NFC-om preko NFC čitača kojeg posjeduje trgovina, [4].

2.3.1. Tipovi mobilnih novčanika

Postoje različite vrste plaćanja putem mobilnog uređaja. Ranijih dana korisnici su koristili mobilne tehnologije koje im omogućavaju pohranjivanje podataka o plaćanju na svoj uređaj zajedno s PIN-om kako bi dovršili transakciju. Mobilni novčanik znatno je olakšao zadatak tako što je korisnicima omogućio pohranjivanje svih podataka o plaćanju, uključujući kreditne kartice, debitne kartice, vaučere i kupone. Postoje 4 glavne vrste mobilnih novčanika koje se dijele na, [4];

- **otvoreno mobilno plaćanje** može se koristiti za kupnju proizvoda, prijenos sredstava putem kartice, podizanje gotovine na bankomatima i sl. Usluge otvorenog novčanika se proširuju u suradnji s ovlaštenim bankama, [4].
- **zatvorene novčanike** izdaju tvrtke za e-trgovinu i tvrtke gdje trgovac zaključava određeni iznos u slučaju vraćanja ili otkazivanja narudžbe. Zatvoreni novčanici mogu se koristiti za kupnju robe i usluga od određenog trgovca. Ova vrsta mobilnog

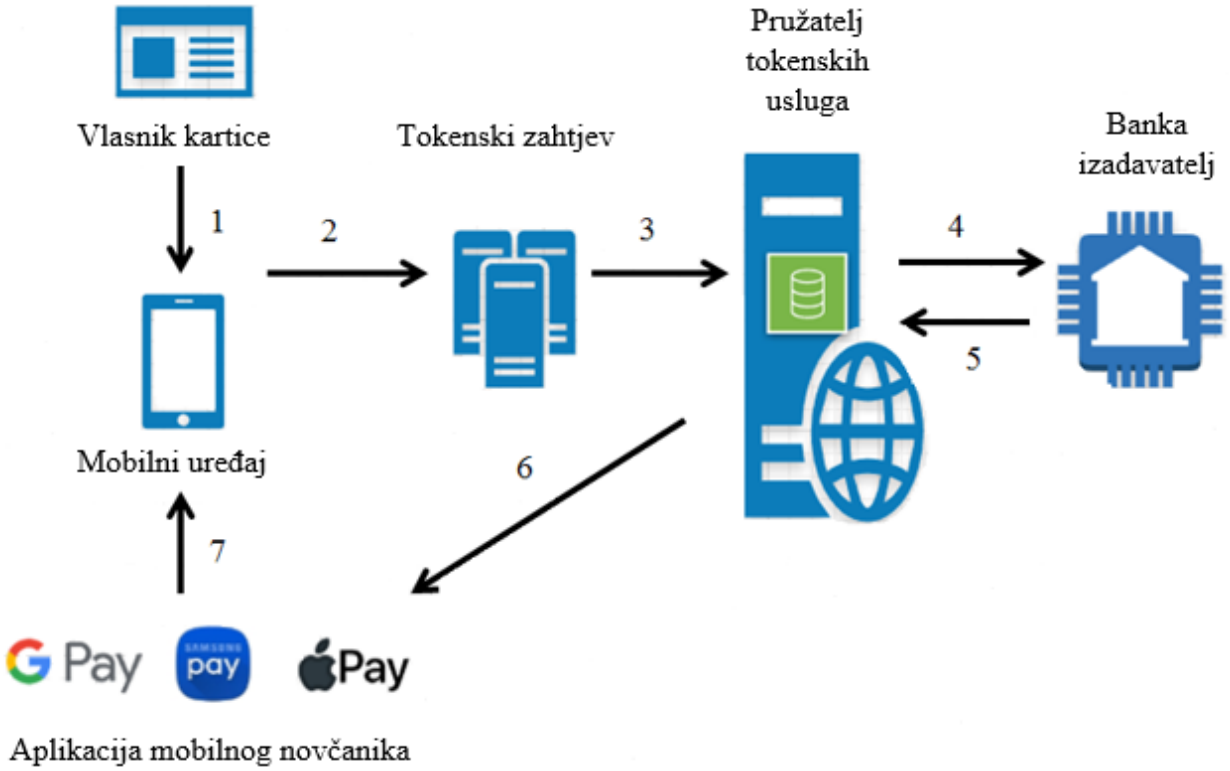
plaćanja ne dopušta podizanje gotovine ili otplatu. Portali za e-trgovinu nude zatvorene novčanike, [4].

- **poluotvoreni sustav plaćanja** omogućava korisnicima da obavljaju transakcije s trgovcima na POS-u koji su povezani s davateljem usluga. Postoje različite vrste aplikacija za mobilno plaćanje poput Apple Pay, Google Pay, Samsung Pay (koji će biti detaljnije opisani u nastavku rada), oni omogućuju korisnicima da plaćaju samo brzim pritiskom otiska prsta. Budući da su sve informacije pohranjene na uređaju, korisnici ne moraju potvrditi datum isteka ili bilo što drugo. Mobilni novčanici zasnivaju se na "push-and-go" proceduri i mogu se koristiti pomoću NFC tehnologije koja je ugrađena u telefon, [4].
- **polu zatvorenu isplate** osiguravaju tvrtke koje su povezane s različitim trgovcima. Ova vrsta mobilnog novčanika omogućava korisnicima obavljanje financijskih transakcija samo na nekoliko lokacija. Nije dozvoljeno podizanje gotovine, [4].

2.3.2. Zaštita mobilnog novčanika

Razmjena novca za robu i usluge uvijek je dolazila s potrebom zaštite. Bez obzira radi li se o gotovini, čekovima, platnim karticama ili kripto kovanicama, ključna je prevencija prijevara. Kad se fokusiramo na platne kartice, tijekom vremena su uvedene brojne metode zaštite. Oni uključuju mehanizme za provjeru autentičnosti vlasnika kartice, poput upotrebe PIN-a, lozinki, raznih biometrijskih zaštita i upotreba podataka magnetske trake pomoću čipa EMV (eng. *Europay, MasterCard and Visa*) te šifriranje podataka s kartice tijekom prijenosa i uporaba tokenizacije, [8].

Tokenizacija je proces zamjene povjerljivih podataka s nepovjerljivim podacima (koji se nazivaju "token"). Ti token podaci jamče istu funkcionalnost, uz dodatnu značajku da nije moguće dobiti ili zaključiti povjerljive podatke na koje su povezani iz samih podataka tokena. Kao u kockarnicama čipovi se zamjenjuju stvarnim novcem. Omogućuju korisniku da se kocka u kockarnici bez potrebe za stvarnim novcem. Ako su žetoni ukradeni, ne mogu se koristiti u drugim kockarnicama. Ovo ograničava polje lopova i ponajviše djeluje kao sredstvo odvraćanja od kriminala. U industriji platne kartice token je nepovjerljiva vrijednost koja se koristi za zamjenu podataka primarnih brojeva.



Slika 3: Dijagram zahtjeva za izradu tokena za plaćanje

Izvor: [8]

Prikazom što sve prolazi jedna transakcija odnosno što se sve događa u pozadini kod izrade tokena za plaćanje nabrojani su koraci i opisana arhitektura (slika 3) kako bi se vidjelo koji su sudionici uključeni u proces izrade tokena i kroz što sve mora proći broj korisnikove kartice kako bi bio zaštićen od napadača i siguran za obavljanje mobilnog plaćanja, [8].

1. Nositelj kartice koristi uređaj koji podržava aplikaciju za digitalne novčanike i registriraju karticu i unose podatke u aplikaciji.
2. Aplikacija podatke šalje tokenskom zahtjevu TR (eng. *Token Request*).
3. TR šalje podatke o pružanju usluge *tokena* TSP (eng. *Token Service Provider*) koji je registriran te je podnio zahtjev za registraciju novog tokena.
4. TSP provjerava podatke kod izdavatelja kartica.
5. Ako je sve ispravno, TSP registrira PAN (eng. *Primary Account Number*) i povezuje ga s novim tokenom u sigurnoj bazi podataka. Uz TR identifikator, datum isteka tokena i niz dodatnih sigurnosnih značajki nazvanih *Token Domain* , uključujući

ograničenja upotrebe novog tokena na određenim kanalima, upotrebu određenog trgovca, ograničenje broja dozvoljenih upotreba i provjere kriptograma.

6. TSP izvještava o primjeni novo generiranog tokena.
7. Aplikacija pohranjuje generirani token (*broj računa uređaja* (DAN) za Apple Pay ili digitalizirani PAN (DPAN) za Samsung Pay) na sigurno mjesto (siguran element (SE) ili emulacija kartice domaćina.

2.3.3. Važni dionici mobilnog novčanika

Mobilni novčanik je virtualni novčanik koji pohranjuje podatke o platnim karticama na mobilni uređaj. Mobilni novčanici korisniku omogućavaju plaćanje u trgovini, a mogu se koristiti kod trgovaca navedenih kod davatelja usluga mobilnog novčanika. Mobilni novčanik je aplikacija koja se može instalirati na pametni telefon ili je već ugrađena kao značajka pametnog telefona. Mobilni novčanik pohranjuje podatke o kreditnoj kartici, debitnoj kartici, kuponima ili nagradnim karticama. Nakon što je aplikacija instalirana i korisnik unese podatke o plaćanju, novčanik pohranjuje te podatke povezujući osobni identifikacijski format poput broja ili ključa, QR koda ili slike vlasnika sa svakom pohranjenom karticom.

Ekosustav mobilnog novčanika čine trgovci koji nude svoje proizvode ili usluge, a da se plaćaju pomoću mobilnog novčanika, zatim banka izdavatelj koja se brine o sigurnosti svih transakcija i provjerava je li korisnik u mogućnosti platiti proizvod ili uslugu. Mobilni novčanik mora biti u mogućnosti ponuditi jedan od načina plaćanja; bankovni račun, pomoću operatora, mobilne mreže, SMS, WAP ili neki drugi oblik.

Također bitan dio mobilnog novčanika je prijenosna mreža preko koje će se slati transakcije, koja mora biti sigurna i zaštićena, to može biti SMS, USSD ili WAP/GPRS. Tehnologija koja se koristi većinom je NFC, ili MST, iako se u budućnosti razmišlja o korištenju QR kodova, *Bluetooth-a* i zvučnih valova kao novijih rješenja. Platna mreža djeluje kao posrednik u mobilnim transakcijama kao i kod cijelog ekosustava mobilnog plaćanja. Mobilni novčanik pokretač je mobilne trgovine pohranjuje korisničke podatke i sprečava ih unositi svaki put kada se izvrši plaćanje. U budućnosti će se mobilne novčanike razvijati u dva smjera, novčanici opće namjene koji koriste NFC mogućnost povezivanja i novčanici s proširenim značajkama kao što je QR / optički kod koji su pogodni i za kupce i za maloprodaju. To će postaviti nove izazove za njihovu funkcionalnu i komponentnu strukturu, što će dovesti do razvoja i poboljšanja njihove arhitekture, [5].

Mobilni novčanik ima sljedeće temeljne funkcije:

- sigurno preuzimanje aplikacije, registracija i pristup u novčanik,
- sigurno pružanje autorizacije (npr. korisničko ime i lozinka),
- zaštita podataka o identitetu korisnika, podataka o plaćanju detalja isporuke,
- odabir načina plaćanja,
- pohranjivanje podataka o različitim brojevima kreditnih i debitnih kartica,
- financiranje iz različitih izvora i
- upravljanje višestrukim mobilnim uslugama plaćanja koje pruža različiti dobavljači, plaćanja od osobe do osobe.

Mobilni novčanik je kombinacija tri komponente: sama komponenta plaćanja, što može biti aplikacija za provjeru autentičnosti plaćanja, njena uloga je osiguranje i provjera platne autentifikacije. Druga komponenta je korisničko sučelje plaćanja koje omogućuje platitelju da upravlja određenim uslugama plaćanja putem prikladnog sučelja, a ovisno o vrsti komponente plaćanja to može biti aplikacija za naplatu putem mobilnih uređaja ili upravitelj vjerodajnica. Treća komponenta jest komponenta korisničkog sučelja koja upravlja spektrom usluga mobilnog plaćanja dostupnog putem mobilnog uređaja, a omogućuje ju izdavatelj mobilnog novčanika, [5].

Potrošačima je sve potrebniji mobilni telefon koji obavlja više funkcija, a mobilni uređaji su se pretvorili u multimedijske uređaje i uređaje s više stotina aplikacija. Jedan od odgovora koji će se dobiti provedbom ankete tijekom ovoga istraživanja jest jesu li krajnji potrošači spremni napustiti novčanik i oslanjati se prije svega na svoj mobilni telefon kao svakodnevni način plaćanja ili su skeptični te i dalje vjeruju uobičajenima kartičnom i gotovinskom plaćanju.

3. NAČINI PLAĆANJA MOBILNIM UREĐAJEM

Ekosustav mobilne tehnologije pruža razne mogućnosti za implementaciju platnih mehanizama. Osnovni GSM (*eng. Global System for Mobile Communications*) mobilni uređaji posjeduje mogućnosti slati i primati informacije (usluge mobilnih podataka) pomoću tri moguća kanala; SMS (*eng. Short Message Service*), USSD (eng. *Unstructured Supplementary Service Data*) ili GPRS (eng. General Packet Radio Service) . Izbor kanala utječe na to na koji će način provoditi usluge mobilnog plaćanja. Aplikacija mobilnog plaćanja može biti smještena na telefonu ili se može nalaziti u modulu identiteta SIM kartice.

Industrija mobilnih plaćanja vrlo je velika i raste po stopi od 60% svake godine. Zbog ovog rasta i potencijala, može se očekivati da će industrija mobilnog plaćanja ispuniti sve veću potražnju korisnika. A tako i vrhunski programeri mobilnih aplikacija stavljaju više resursa u ovoj domeni jer nude razna aplikacijska rješenja i načine mobilnog plaćanja. Mobilno plaćanje razvija se brzim tempom, gdje mnogo novih načina i brendova ulazi u industriju. U ovoj cjelini spomenut će se najkorišteniji i najpopularniji načini mobilnog plaćanja te njihove prednosti, funkcije i nedostatci.

3.1. SMS plaćanja

SMS plaćanja ili plaćanja putem teksta su način plaćanja usluga ili robe putem SMS poruke s mobilnog telefona. Kupac obično prima tekst kojim se na neki način poziva da pokrene plaćanje putem web sučelja ili dodatnih tekstualnih poruka. Gotovo svaka tvrtka koja uzima plaćanja za robu ili usluge može ostvariti uštedu operativnih troškova i povećati prikupljeni prihod odabirom SMS plaćanja.

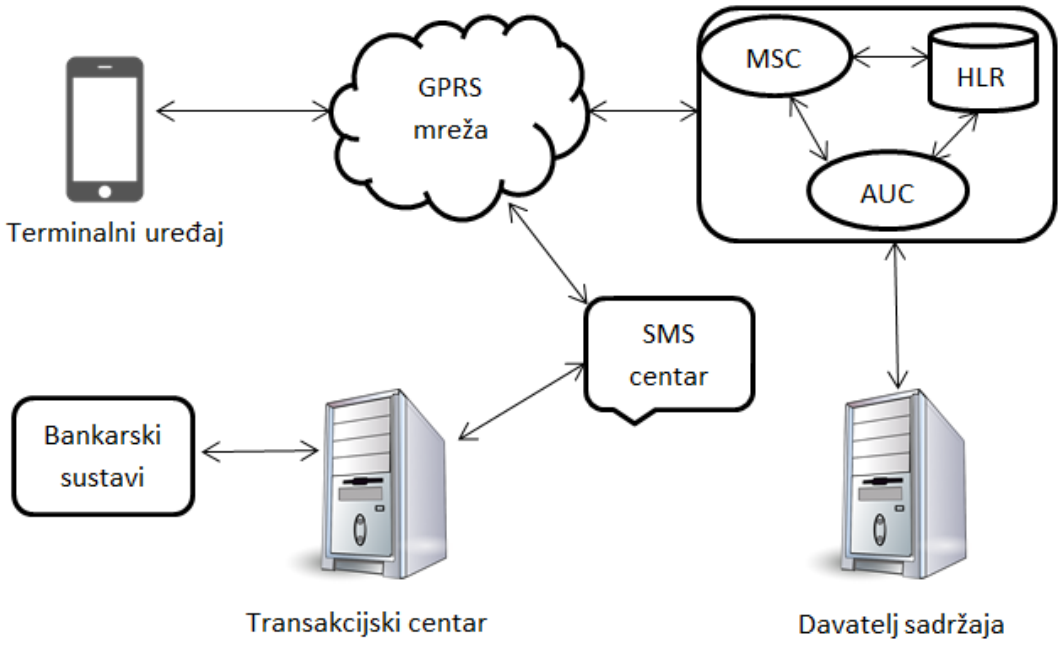
Prednosti SMS plaćanja za kupce:

- SMS plaćanja su brza i jednostavne za korištenje,
- SMS i bez plaćanja ima sigurno okruženje,
- ne moraju se plaćati računi putem uplatnice u banci ili pošti,
- ne objavljuju se osobni podaci ili detalji računa,
- kupci ne otkrivaju osjetljive informacije o sebi,
- kupac ne mora unositi svoje kreditne kartice ili bankovne podatke, pa čak ni imati bankovni račun i

- kupci ne trebaju pamtiti lozinke ili korisnička imena poput web mjesta poput Pay Pala.

Prednosti SMS plaćanja za posao

- trgovac može prihvatiti plaćanja s bilo kojeg od milijardi mobilnih telefona koji mogu slati SMS-ove širom svijeta,
- jednostavan za korištenje,
- poboljšano zadovoljstvo kupaca,
- trgovci mogu primati plaćanja od kupaca bez bankovnog računa ili kreditne kartice,
- može se graditi na lojalnosti kupaca kroz: SMS marketinške poruke, popuste, kupone, provjera identiteta kupaca, praćenje plaćanja,
- smanjenje broj kašnjenja u plaćanju i brža naplata,
- uklanja ljudsku pogrešku prilikom ručne obrade i
- potiče potrošače da ne moraju plaćati gotovinom.



Slika 4: Standardni format slanja SMS poruke za plaćanje usluge

Izvor: [9]

Način na koji funkcioniraju SMS plaćanje je jednostavno (slika 4). Iako možda postoje neke varijacije kod svake tvrtke koja nudi usluge plaćanja SMS-om, općenito se može očekivati sljedeće elemente kada dođe vrijeme za plaćanje, [9]:

1. Tvrtka šalje tekst na telefonski broj svog kupca ili kupac šalje kratki kod tvrtki kako bi pokrenuo prodaju.
2. Nakon što je priopćio koji proizvod ili uslugu kupac želi kupiti, tvrtka šalje kupcu vezu do sigurnog mobilnog oblika plaćanja.
3. Kupac unosi svoje podatke o plaćanju i obično može odobriti spremanje kartice na datoteku za ponavljajuća plaćanja ili buduću kupnju.
4. Kupac može dobiti jedinstveni kod za dovršetak kupnje.
5. Kupac može dobiti i drugi potvrdni tekst od tvrtke za obradu plaćanja kako bi potvrdio svoju namjeru kupnje. Kao što je gore navedeno, točan postupak može se razlikovati od tvrtke do tvrtke.

3.2. Plaćanje korištenjem WEB servisa

Mnogi ljudi jednostavno plaćaju putem WEB-a (eng. World Wide Web jedna od najkorištenijih usluga Interneta koja omogućava pregled hipertekstualnih dokumenata) u svom pregledniku mobilnog uređaja (npr. *Samsung Internet*, *Chrome*) ili unutar aplikacija, pod uvjetom da postoji Wi-Fi ili mobilna mreža (3G /4G). Postoji nekoliko načina za plaćanje na ovaj način. Može se ručno unijeti podatke o kartici na *web* mjestu kako bi se platila narudžba, tako da se automatski koristi bankovnu karticu u prilogu mobilne aplikacije, može se koristiti u kombinaciji s PayPal-om ili slijedili vezu do digitalne transakcije koja je poslana u pregledniku.

S obzirom na to da pametni telefoni mogu pristupiti cijelom Internetu, ljudi jednostavno unose podatke sa svoje kartice na stranicu za odlazak na *web* mjesto kako bi dovršili plaćanje. Kada unesu podatke kod većine kartica prilikom korištenja ovakvog način plaćanja potrebno je imati i aplikaciju mobilnog bankarstva jer zbog sigurnosti plaćanje neće biti moguće, kao što je primjer kod m-zaba (aplikacijsko rješenje za mobilno bankarstvo Zagrebačke banke) aplikacije nakon unesenih podataka o kartici korisniku se otvara prozor za unos tokena za plaćanje, kako bi se transakcija obavila sigurno i bez rizika od izlaganja povjerljivih informacija napadaču. Prije 2010. godine ovo se obično nazivalo plaćanja putem protokola bežične aplikacije WAP (eng. *Wireless Application Protocol*). WAP je nekada bio najčešći program na pametnim telefonima

koji se povezuju s internetom. Umjesto *web* preglednika s pristupom cijelom internetu, ljudi su plaćali putem WAP preglednika ili aplikacije ograničenog kapaciteta zajedno klasificirane kao WAP plaćanja. Danas je tu tehnologiju zamijenilo Internet plaćanje.

Jedan od primjera web plaćanja jest *Paysafecard* koja je jedna od vodećih tvrtki na globalnom tržištu web plaćanja. Pomoću nje se može plaćati na stranicama različitih web trgovina bez potrebe za bankovnim računom ili kreditnom karticom. Paysafecard funkcionira jednostavno, prvo korisnik pomoću tražilice pronađe najbliže prodajno mjesto koje koristi ovakvu vrstu usluge mobilnog i wrb plaćanja (većinom su to benzinske pumpe i veća prodajna mjesta), drugi korak se sastoji od toga da kad korisnik pronađe prodajno mjesto i tamo kupi *paysafecard* PIN (korisniku je na raspolaganju da bira između PIN-ova od 50 kn,100 kn, 200 kn, 350 kn i 500 kn), nakon što je odabrao PIN i dobio odgovarajući 16 znamenkasti kod korisnik može otvoriti svoj preglednik na mobilnom uređaju i platiti nešto online u tisućama web trgovina (slika 5) samo unosom koda kojeg je prethodno kupio pomoću Paysafecard aplikacije. Zanimljivo i inovativno rješenje kod ovakvog načina mobilnog plaćanja jest ako korisnik plati proizvod ili uslugu manje nego što mu je iznos sredstava koje je kupio prethodno, korisnik je i dalje u mogućnosti koristiti isti 16 znamenkasti kod sve dok ne potroši sva sredstva koja je uzeo preko PIN-a Paysafecard-a, [10].

Slika 5: Prikaz 3 jednostavna koraka prilikom plaćanja paysafecard PIN kodom

Izvor: [10]

3.3. Bluetooth plaćanje

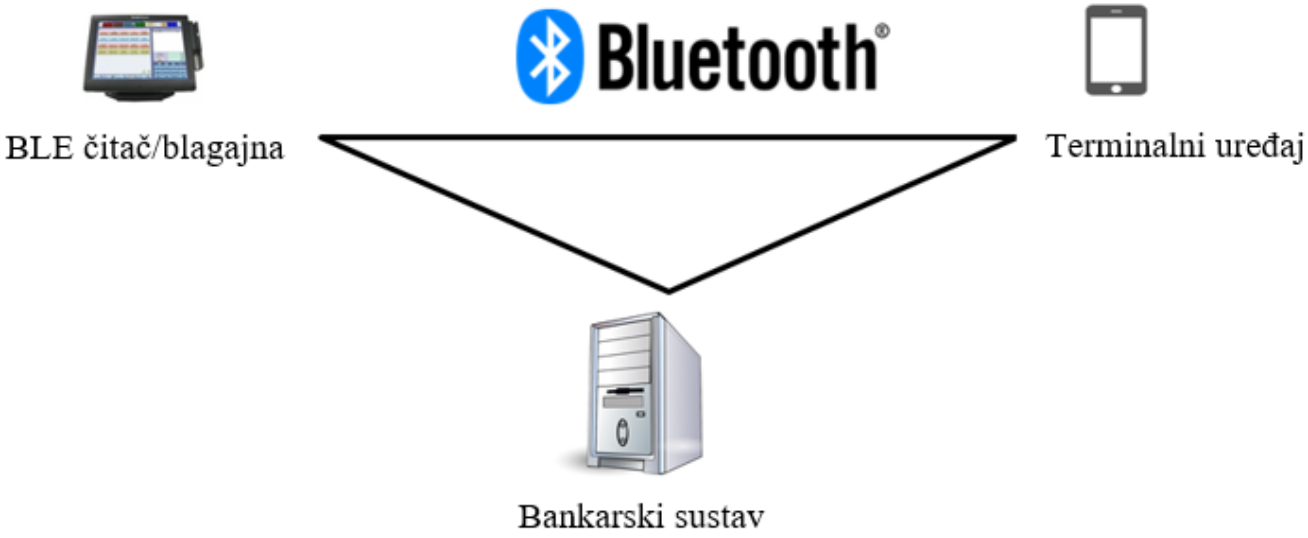
Mobilna plaćanja koja koriste *Bluetooth* oslanjaju se na radio valove za prijenos informacija. Za plaćanje putem mobilnih uređaja programeri *Bluetooth* stvorili su senzore koji troše malo baterije. Kako ovi senzori troše manje energije nego inače, standard za plaćanje

putem mobilnih uređaja poznat je pod nazivom BLE (eng. *Bluetooth Low Energy)*. BLE standard prihvaćen je u mobilnoj industriji Apple, Android, Windows i BlackBerry. Za razliku od ostalih standardnih plaćanja putem mobilnog telefona, kod korištenja mobilnog plaćanja putem Bluetooth tehnologije nije potrebno vaditi uređaj iz džepa. BLE radi na udaljenosti do 50 metara, tako da kupac može samo proći pored blagajne, a sustav prodajnih mjesta povezao bi se s mobilnim uređajem i preuzeo podatke o kupcu te naplatio određeni iznos koji je potrebno platiti. Plaćanje BLE tehnologijom ima nekoliko prednosti nad plaćanjem NFC tehnologijom, [11]:

- za plaćanje BLE tehnologijom potrebno je 0.003 sekundi, dok je za plaćanje NFC tehnologijom potrebno 0.1 sekunda i
- za plaćanje BLE tehnologijom korisnik nema potrebu čekati u redu za plaćanje u dućanu odnosno nema potrebu staviti terminalni uređaj u ruku za razliku od plaćanja NFC tehnologijom gdje korisnik fizički mora približiti terminalni uređaj POS uređaju i čekati u redu za plaćanje,

Nedostaci plaćanja BLE tehnologijom nad NFC tehnologijom su sljedeće, [11]:

- plaćanje NFC tehnologijom je način plaćanja koji je mnogo rasprostranjeniji nego plaćanje BLE tehnologijom i
- opasnost od napada MTM (engl. *Man in The Middle*) odnosno presretanja podataka o plaćanju između terminalnog uređaja do uređaja za plaćanje. S obzirom na to da je preporučeni domet plaćanja BLE tehnologijom do pedeset metara, navedeni napad je moguć.



Slika 6: Plaćanje BLE tehnologijom

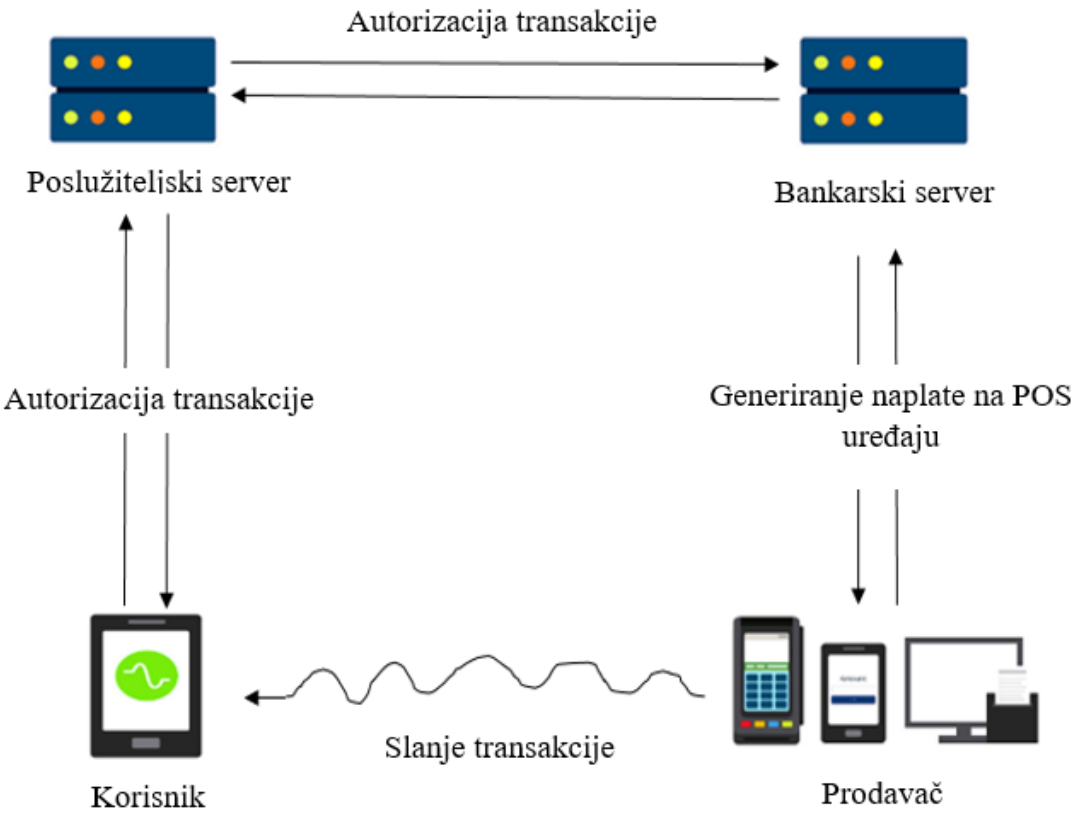
Izvor: [11]

Korisnik koristeći BLE tehnologiju se spaja s blagajnom prodavaonice koja sadrži BLE čitač signala za plaćanje (Slika 6). Prijenosom informacija prema blagajni, terminalni uređaj odnosno aplikacija koja se koristi za plaćanje šalje informacije prema banci korisnika za provedbu plaćanja, nakon čega bankarski sustav šalje novčani iznos prema računu prodavaonice, [11].

3.4. Isplate temeljene na zvučnim valovima

Mobilno plaćanje zasnovano na zvučnom valu (ili zvučni signal) predstavlja novije, vrhunsko rješenje koje djeluje na većini mobilnih telefona. Transakcije se obrađuju bez potrebe za internetom jedinstvenim zvučnim valovima koji sadrže šifrirane podatke o plaćanju. Zvučni valovi šalju se s terminala na mobilni telefon kako bi prenijeli detalje o plaćanju, gdje korisnikov mobilni uređaj pretvori te podatke u analogne signale koji dovršavaju transakciju. Umjesto korištenja ugrađene tehnologije poput NFC-a, mobilni novčanik, bankarska aplikacija ili terminal kartice jednostavno treba instalaciju softvera. Nema potrebe za dodatnim hardverom. To ga čini pristupačnim rješenjem, posebno u područjima i zemljama u kojima si ljudi ne mogu priuštiti najnovije pametne telefone, ali se oslanjaju na više osnovne tehnologije za obradu plaćanja.

Tehnologija zvučnih valova radi na financijskoj inkluziji omogućujući svim vrstama telefonima da izvrše digitalna plaćanja. Budući da je softverski element, on se može lako integrirati u postojeći hardver, što ga čini isplativim. Svojim rješenjem tehnologija zvučnih valova je uključiva i može pomoći zemljama u razvoju kao i tehnološki naprednim zemljama da se uhvate u korak s drugim zemljama i njihovim ekonomskim politikama prema bezgotovinskom plaćanju. Ova tehnologija koristi zvučnik i mikrofon mobilnog uređaja kao medij za komunikaciju s POS-om za obavljanje plaćanja. To je slično načinu na koji Bluetooth uređaj zahtijeva Bluetooth hardver, WiFi-u treba usmjerivač, a NFC-u trebaju dva NFC uređaja. To je u osnovi softver koji se može instalirati u bilo koje trgovačke aplikacije koje olakšavaju digitalno plaćanje. Pomoću aplikacije potrošači mogu kliknuti ikonu plaćanja na kojoj trgovac prima skočni prozor da prihvati plaćanje. To se vrši pomoću zvučnih valova. Slično je i s drugim načinima digitalnog plaćanja u kojima potrošač može identificirati trgovca prema svom telefonskom broju ili barkodu, [12].



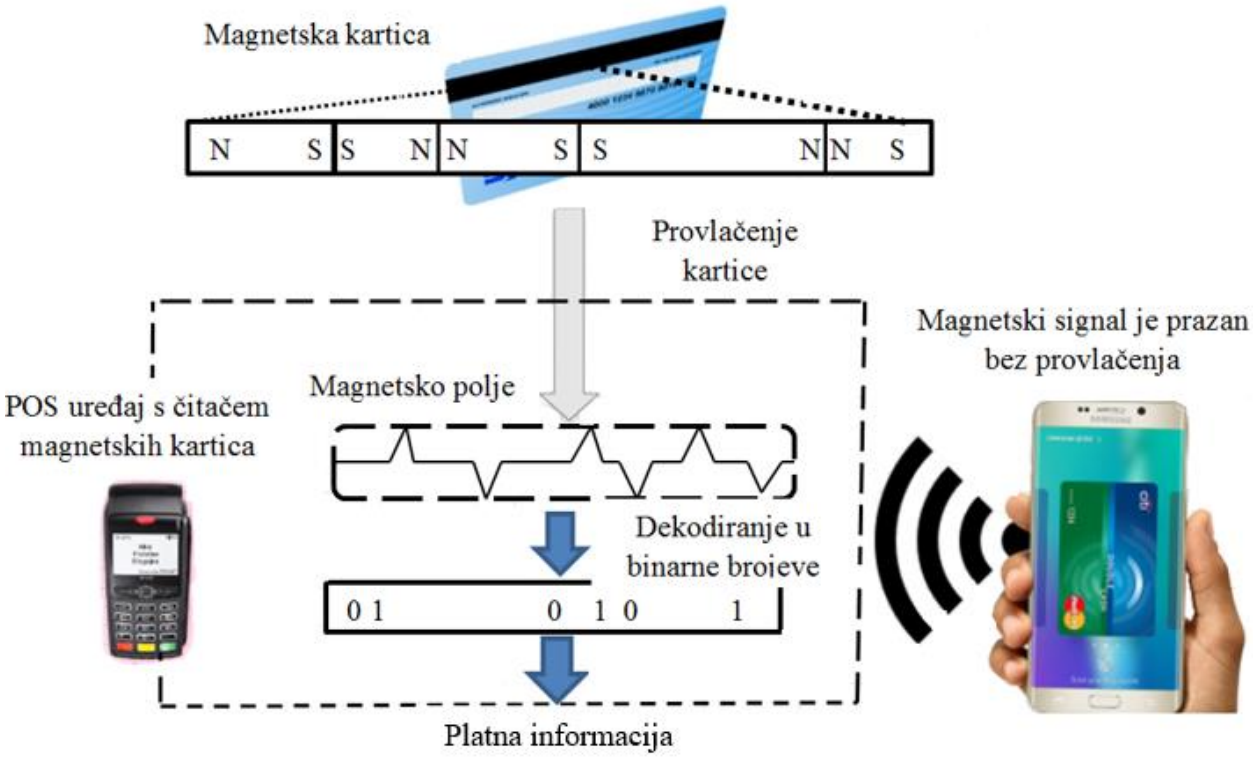
Slika 7: Sigurni tijek transakcije ToneTag

Izvor [17]

Kada govorimo o plaćanju pomoću zvučnih valova neizostavno je spomenuti aplikacijsko rješenje ToneTag budući da za prijenos podataka koristi zvučne valove, tehnologija ToneTag omogućava plaćanja koja su neovisna o bilo kojem instrumentu. To znači da plaćanja ne ovise o određenom hardveru. Također oni ne ovise o internetskoj povezanosti. Trgovac može programirati bilo koji uređaj na mobilni telefon, POS uređaj ili koristiti ToneTag uređaj i prenijeti iznos računa i pojedinosti o transakciji putem zvučnog signala. Korisnici mogu autentificirati plaćanja putem svojih telefona (slika 7). Ova tehnologija omogućuje da se transakcije dovrše kada su dva uređaja u neposrednoj blizini. ToneTag osigurava sigurnost podataka koristeći kriptiranje podataka te tako čine transakcije sigurnijima od transakcija na kartici. Može se integrirati i s digitalnim novčanikom i aplikacijama za plaćanje. Tehnologija također može raditi na bilo kojem operacijskom sustavu iOS, Android, Windows i Linux te ne mora biti nužno pametni telefon da bi funkcionirao, [17].

3.5. Plaćanja magnetskim sigurnim prijenosom (MST)

Magnetski siguran prijenos MST (eng. *Magnetic Secure Transmission*) naziv je tehnologije za mobilno plaćanje u kojoj uređaji poput pametnih telefona emitiraju signal koji oponaša magnetsku traku na tradicionalnoj platnoj kartici. MST šalje magnetski signal s uređaja na čitač kartica terminala za plaćanje. Tako se oponaša prevlačenje fizičke kartice bez potrebe za nadogradnjom softvera ili hardvera terminala za podršku naprednije tehnologije poput beskontaktnog plaćanja. Za razliku od NFC plaćanja MST tehnologija je kompatibilna s gotovo svim terminalima za plaćanje koji imaju čitač magnetske trake. Izvorni MST oponašao je tehnologiju nešifrirane magnetske pruge kako bi bio kompatibilan sa starijim terminalima kreditnih kartica, bežični prijenos nije šifriran i stoga se ne smatra sigurnim. Kad prodajno mjesto ima blagajničke terminale telefon se ne može predati na blagajni kao što je kreditna kartica jer za mobilno plaćanje se mora koristiti otisak prsta. Još uvijek postoje mnoga prodajna mjesta koje prihvaćaju samo gotovinu. Tako da je ovaj način mobilnog plaćanja još ne koristi intenzivno, ali svakako predstavlja jedan od načina plaćanja koji bi se mogli koristiti u budućnosti, [13].



Slika 8: Prikaz klizanja karata MST u Samsung Payu

Izvor: [13]

Prikazom uobičajenog scenarija za off-line plaćanje pomoću kreditne kartice i usporedbom s MST (slika 8) koji radi tako da se prebaci kreditna kartica u čitaču kartica i generira se magnetski signal. Dok čitač kartica može prepoznati podatke o plaćanju u kartici dešifriranjem podataka u magnetskom signalu. MST uređaj na daljinu generira takav magnetski signal i prosljeđuje ga u čitač kartica koji zatim prepoznaje signal, to se ostvaruje tako da korisnik provlači mobitel pored POS uređaja te se tako generira MST signal, a POS uređaj dekodira taj signal u binarne brojeve i na kraju se dobiva platna informacija.

3.6. Plaćanje QR kodom

QR kodovi su kvadratni bar kodovi. QR (eng. *Quick Respond*) crtični kodovi dizajnirani su tako da sadrže značajne informacije pravo na crtični kod (slika 9). QR kodovi mogu biti dvije glavne kategorije: QR Code predstavljen je na mobilnom uređaju osobe koja plaća i skenira putem POS-a ili drugog mobilnog uređaja primatelja ili QR kod prima primatelj na statički ili jednokratni način, a skenira ga osoba koja izvršava plaćanje.

Prednosti plaćanja QR kodom jesu, [18];

- jednostavna primjena - razmjena je relativno brza i jeftina,
- pouzdanost - podaci o plaćanju, naslov i iznos automatski se popunjavaju, nema grešaka,
- mobilne aplikacije koje posjeduju QR kodove nude najviše standarde sigurnosti i zaštite podataka i
- tržište koje se može adresirati - budući da se NFC čip zahtijeva na telefonu, adresabilno tržište za ovo tehnološko sučelje je prilično veliko.

Slika 9: Prikaz plaćanja QR kodom

Izvor: [18]

3.7. Plaćanje NFC tehnologijom

NFC je skup komunikacijskih protokola za komunikaciju između dva elektroničkih uređaja na udaljenosti od 4 cm ili manje. NFC nudi vezu s malim brzinama jednostavnog postavljanja koja se može koristiti za pokretanje bežičnih veza s više mogućnosti. Koriste se u beskontaktnim platnim sustavima i omogućuju zamjenu ili dopunu mobilnog plaćanja kao što su kreditne kartice i pametne kartice. NFC se može koristiti za dijeljenje malih datoteka poput kontakata i pokretanje brzih veza za dijeljenje većih medija kao što su fotografije, videozapisi i druge datoteke. NFC tehnologija omogućuje bežično povezivanje uređaja u kratkom dometu pritom koristeći magnetsku indukciju polja za ostvarivanje komunikacije između istih uređaja. Tehnologija omogućuje visoku frekvenciju, nisku propusnost i standardizaciju bežičnih komunikacijskih tehnologija. Razvojem pametnih mobilnih uređaja zamjenjuje se beskontaktna kartica. Uređaji djeluju kao beskontaktna kartica (na temelju njegovog sigurnosnog elementa) i kao beskontaktni čitač koji također djeluje u P2P modu s uređajima koji također to podržavaju, [9].

Mobilno plaćanje NFC tehnologijom je proces transakcije novčanih sredstava na drugi račun koristeći NFC tehnologiju na terminalnom uređaju. Sigurnosni elementi koji se nalaze unutar SIM kartice ili čipa terminalnog uređaja zaštićeni su od napada od strane napadača višeslojnom zaštitom kako bi se proces transakcije novčanih sredstava proveo na siguran način. Mobilno plaćanje nije moguće ako su u terminalnom uređaju otvorene mogućnosti korištenja operativnih postavki koje inače nisu dostupne vlasniku (*root* pristup uređaju) jer navedeno aplikacija prepoznaje i brani korisniku plaćanje preko terminalnog uređaja kako bi ga zaštitila od izlaganja podataka u slučaju da je terminalni uređaj zaražen malicioznim kodom, unatoč višeslojnoj zaštiti sigurnosnih elemenata u SIM kartici ili čipu unutar terminalnog uređaja, [9].

3.7.1. Vrste NFC komunikacije

Uz tehnologiju signalizacije koju koristi NFC, postoje četiri vrste oznaka. Vrste oznaka odnose se na brzinu i kompatibilnost između NFC oznake i NFC čitača, a uloge određuju kako aktivni i pasivni uređaji reagiraju tijekom komunikacije. URL (eng. *Uniform Resource Locator)* u prijevodu ujednačeni ili usklađeni lokator sadržaja resursa koji je najčešće i ugrađen u NFC oznaku, zauzimaju samo malo memorije smanjujući troškove proizvodnje NFC oznaka.

Vrste NFC oznaka, [15]:

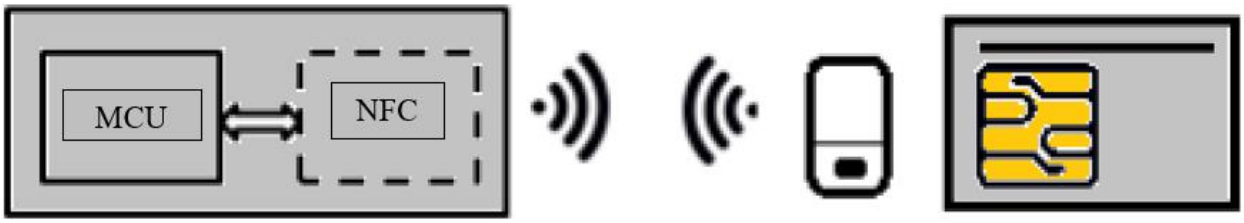
- tip 1 : Oznake NFC tipa 1 imaju zaštitu od sudara podataka i mogu se postaviti na mogućnost čitanja i prepisivanja s mogućnošću samo za čitanje ili samo za pisanje. Programiranje samo za čitanje sprečava da se informacije promijene ili prepisuju nakon što su jednom ugrađene u oznaku. Oznake tipa 1 imaju 96 bajtova memorije, dovoljno za URL ili malu količinu podataka. Memorija oznake može se prema potrebi proširiti na veću količinu. Niska cijena čini oznake tipa 1 idealnim izborom za većinu komunikacijskih protokola u blizini,
- tip 2 : NFC oznake tipa 2 također imaju zaštitu od sudara podataka i mogu se prepisati ili samo za čitanje. Započinju s 48 bajtova memorije, polovinom onoga što mogu sadržavati oznake tipa 1, ali mogu se proširiti i do oznake tipa 1. Brzine komunikacije iste su za tipove 1 i 2,
- tip 3 : Također opremljen zaštitom od sudara podataka, NFC oznaka tipa 3 ima veću memoriju i veće brzine od oznaka tipa 1 i 2.. Veličina omogućuje držanje složenijih kodova osim URL-ova, ali košta više izrade svake oznake i
- tip 4 : NFC oznake tipa 4 mogu koristiti ili NFC-A ili NFC-B komunikaciju i imati zaštitu od sudara podataka. Oznaka je postavljena kao prepisiva ili samo za čitanje, a proizvodi ne mogu promijeniti te postavke, za razliku od ostalih NFC oznaka koje se kasnije mogu promijeniti. Oznaka drži 32 kB u memoriji i ima veće brzine od ostalih oznaka.

NFC se može koristiti na tri različita načina, [9]:

- peer-to-peer: dva uređaja s omogućenom NFC-om mogu uspostaviti vezu i dijeliti podatke,
- čitanje / pisanje: Aktivni uređaj poput telefona skuplja podatke s pasivnog uređaja koji nema mogućnost samog čitanja podataka i
- emulacija kartice: NFC uređaj može se koristiti poput beskontaktne kreditne kartice.

Treća je upotreba ona koja se najviše primjenjuje na trgovce jer omogućava prihvaćanje plaćanja putem mobilnog novčanika predstavlja i glavni dio istraživanja s obzirom na to da je fokus rada mobilno plaćanje. Način rada s emulacijom kartice se temelji na tome da se NFC terminalni uređaj ponaša kao beskontaktna pametna kartica koja ne generira svoje radio frekvencijsko polje već radio frekvencijsko polje generira NFC čitač. Sve dok mobilne platforme

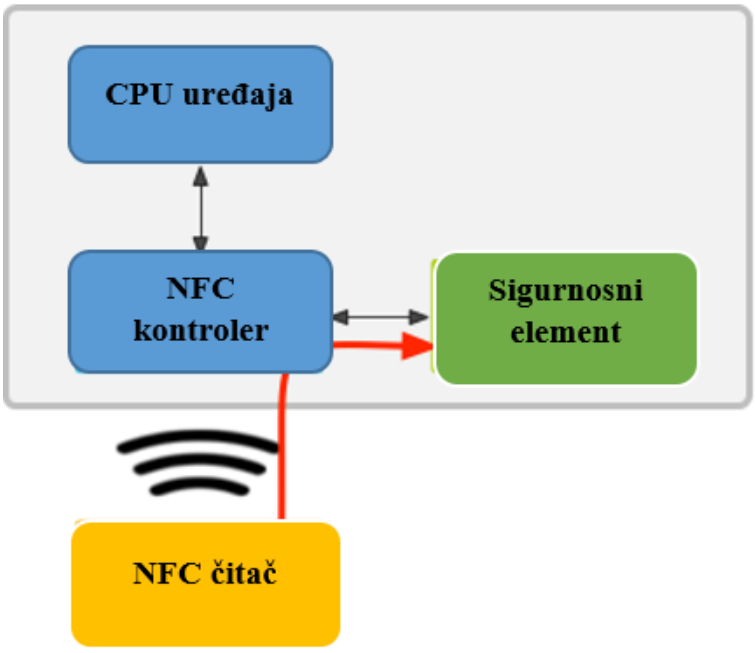
podržavaju emulacijski protokol kojeg koriste regularne beskontaktne kartice, moći će se koristiti emulacijski način rada. U ovom načinu rada, mobilni uređaj se može koristiti kao kreditna ili debitna kartica tako da korisnik nema potrebu nositi sa sobom fizičku beskontaktnu karticu, [9].



Slika 10: NFC emulacija kartice

Izvor: [9]

Mnogi uređaji sa sustavom Android koji nude NFC funkcionalnost već podržavaju emulaciju NFC kartice (slika 10). U većini slučajeva kartica se oponaša zasebnim čipom u uređaju, koji se naziva sigurnim elementom. Mnoge SIM kartice koje također sadrže siguran element. Sve osjetljive informacije čuvane su u sigurnom elementu na EMV (ranije objašnjeno značenje kratice) karticama odnosno čipu koji samo komunicira s čitačem kartica. Sigurni element omogućuje nekoliko funkcija uključujući kriptografsku provjeru za validaciju integriteta kartice i verifikaciju vlasnika preko PIN-a.



Slika 11: Emulacija kartice sa sigurnosnim

Izvor: [16]

Kada se izvrši mobilno plaćanje korištenjem SIM kartice sa sigurnim elementom NFC čitač komunicira direktno sa sigurnim elementom (Slika 11) i nijedna Android aplikacija nije uključena u transakciju u bilo kom smislu. Kada se transakcija završi Android aplikacija dobiva mogućnost provjere za status transakcije i obavještava korisnika. Sigurni element služi kao čip u EMV karticama, [16].

3.7.2. Sigurnost plaćanja NFC tehnologijom

Mobilni novčanici su sigurniji od kartica s magnetskim trakama. Iako je telefon još uvijek podložan krađi, sve dok je aktiviran pristupni kod ili biometrijska zaštita lopovima će uređaj biti gotovo beskoristan. Uz mobilne novčanike podaci o plaćanju potrošača izlažu se samo jednom i to kada se podaci o kartici unesu u mobilni novčanik. Ti se podaci zatim šifriraju tako da svaki put kada kupac koristi svoj mobilni novčanik šalju se virtualni podaci o plaćanju (što znači ne stvarni podaci o kartici). Puni broj kartice nije izložen, a kada se virtualni podaci proslijede na terminal za plaćanje trgovački proces plaćanja često ga odmah šifrira provjerenim metodama platne kartice. Beskontaktna rješenja za plaćanje djeluju na nevjerojatno kratkim udaljenostima (govorimo o centimetrima). Da bi potencijalni kradljivac mogao ukrasti podatke morao bi stajati neugodno u blizini uređaja s omogućenom NFC-om. Ova zaštita od blizine predstavlja prvu razinu obrane. Da bi započeo svaku transakciju kupac mora aktivno pokrenuti postupak beskontaktnog plaćanja. To obično zahtijeva pokretanje odgovarajuće NFC aplikacije unutar telefona kako bi se uspostavila veza između uređaja i čitača POS uređaja trgovca. Čak i ako se kradljivac dovoljno približi ne mogu se dogoditi nikakve transakcije, [16].

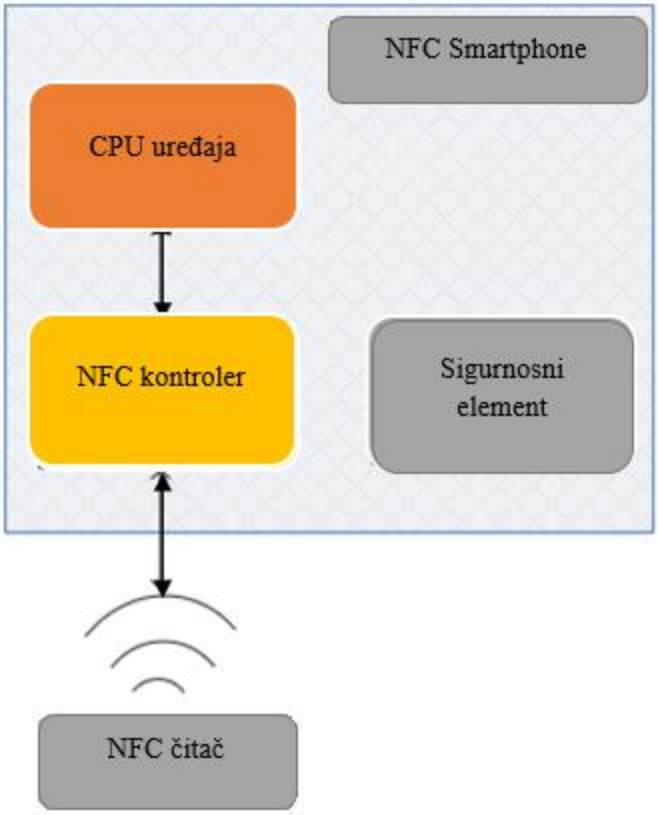
Jednom kada se uspostavi veza, transakcija prolazi tek nakon što kartica ili mobilni uređaj potvrdi kupnju pomoću čipa sigurnog elementa. Ovaj postupak provjere dodjeljuje jedinstveni digitalni potpis svakoj uplati umjesto prijenosa brojeva kreditne ili debitne kartice između uređaja i čitača. Napadač ne treba uzimati svaki pojedinačni signal za prikupljanje privatnih podataka. Dvije metode mogu spriječiti prisluškivanje. Prvo je sam raspon NFC-a budući da uređaji moraju biti prilično blizu za slanje signala, napadač ima ograničen domet za presretanje signala. Zatim postoje sigurni kanali, kad se uspostavi siguran kanal podaci se kriptiraju i samo ih ovlašteni uređaji mogu dešifrirati. Krađa podataka i manipulacija događaju se kada napadač manipulira podacima koji se šalju primatelju ili ometa podatke koji se šalju tako da su oštećeni i beskorisni kada stignu na odredište. Za komunikaciju treba koristiti sigurne kanale. Nijedna

količina šifriranja ne može zaštititi potrošača od ukradenog telefona. Ako je ukraden pametni telefon napadač bi teoretski mogao mahati telefonom preko čitača kartica u trgovini kako bi obavio kupnju. Da bi se to izbjeglo vlasnici pametnih telefona trebali bi biti oprezni te održavati strogu sigurnost na svojim telefonima. Instaliranjem lozinke ili druge vrste zaključavanja koja se pojavljuju kada je zaslon pametnog telefona uključen, lopov možda neće moći shvatiti lozinku i stoga ne može pristupiti osjetljivim informacijama na telefonu, [16].

3.8. HCE Tehnologija

Kao najperspektivniji način rada NFC-a spomenut je način emulacije kartice koji omogućuje uređaju da oponaša beskontaktnu pametnu karticu. Način emulacije kartice podržava realizaciju različitih aplikacija poput mobilnog plaćanja, kupnje karata, kupona, kontrole pristupa, identifikacije i tako dalje. U ovom je načinu SE (*eng. Secure Element)* sigurnosni element središnje područje aktivnosti koje je definirano kao područje na NFC pametnim telefonima za sigurno pohranjivanje osjetljivih podataka (npr. kreditne kartice i identifikacijski broj) potrebnih za obavljanje NFC transakcije. Do danas je predloženo nekoliko opcija SE, uključujući SE bazirane na UICC (eng. *Universal Integrated Circuit Cards*), ugrađeni SE bazirani na hardveru SE, SD (eng. *Secure Digital*) sa SE softverom. Stoga je postizanje pravednog rješenja među dionicima u ovom složenom ekosustavu od najveće važnosti, [22].

Koncept SE utemeljen na oblaku pojavio se uvođenjem tehnologije emulacije ***Host Card Emulation*** (**HCE**) u Android 4.4 (KitKat) OS (operativni sustav). HCE tehnologija razdvaja funkcionalnost emulacije kartice od hardverske SE i pruža virtualni prikaz osjetljivih podataka. HCE koristi mobilni OS kako bi omogućio virtualni SE u oblaku kao udaljeno okruženje. Ekosustav HCE tehnologije čine dvije strane kako bi se provela transakcija između trgovca i banke, zaobilazeći sustav mobilnog operatora. Sigurnosni elementi se ne nalaze unutar terminalnog uređaja i nisu vezani uz mobilnog operatora već se nalaze u oblaku (*Cloudu*) koji su dostupni preko Interneta. *Smartphone* (pametni telefon) i dalje obavlja funkcije emulacije kartice, ali privatni podaci se pohranjuju, osiguravaju i pristupa im se u Cloudu. Navedena prednost ne znači previše za korisnika koji plaća, ali je za programere i vlasnike mobilnih novčanika značajna i lakše im je za korištenje te predstavlja budućnost, [22].



Slika 12: HCE komunikacijski tijek

Izvor: [22]

HCE tehnologija funkcionira tako da zahtjeva pristup procesoru terminalnog uređaja kako bi se provela transakcija odnosno pristup sigurnosnim elementima koji se nalaze u *Cloud-u* preko Interneta, a ne u SIM kartici ili čipu kao što je slučaj kod NFC tehnologije. Kako bi podaci odnosno sigurnosni elementi bili sigurni od krađe koristi se proces pretvaranja podataka sigurnosnih elemenata u niz nerazumljivih slova ili znamenka sve do odredišta odnosno bankarskog sustava gdje se vraćaju u prvobitno stanje, [9].

Svrha i cilj uvođenja koji stoje iza HCE tehnologije je njegova neovisnost od hardverskih rješenja utemeljenih na SE. U slučaju hardverski utemeljenih SE naredbe primljene od NFC čitača šalju se aplikaciji na SE pametnog telefona uz pomoć NFC kontrolera, tako da SE obrađuje naredbe i šalje odgovore. Dok u slučaju HCE tehnologije primljene naredbe NFC kontroler prosljeđuje u aktivnu aplikaciju NFC kao što je prikazano (slika 12), a mobilna aplikacija obrađuje naredbe primljene od NFC čitača. S obzirom na računalni kapacitet, kapacitet pohrane, složenost implementacije i trošak pohrane svih podataka koji se obavljaju u

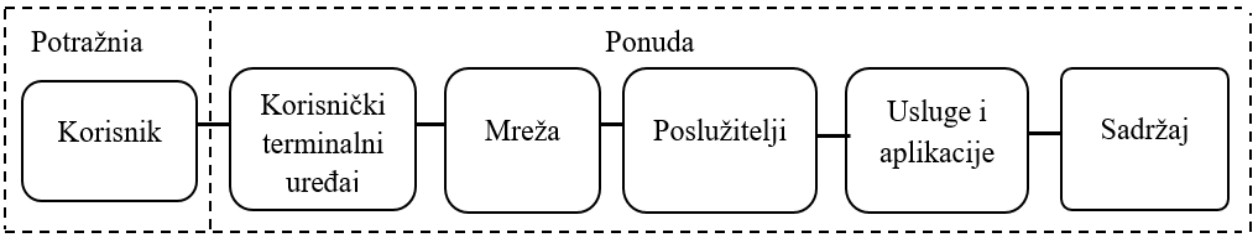
određenom ekosustavu mobilnog plaćanja dolazi se do zaključka da su NFC usluge temeljene na HCE povoljnije u usporedbi s hardverskim SE. U pogledu NFC ekosustava i poslovnih modela rješenja temeljena na HCE neovisna su od; davatelja usluga, TSM-a, mobilnog operatora i dr. sudionika ovisnih o hardveru te infrastrukturi, stoga se HCE tehnologija može smatrati mjenjačem igre koji će učiniti NFC dostupnijim i svestranijim za programere i krajnje korisnike. Na ostalim sudionicima je da nađu rješenje kako će se uklopiti u takav novi način funkcioniranja NFC-a i cijelog ekosustava mobilnog plaćanja temeljenog na HCE tehnologiji, [22].

4. ANALIZA EKOSUSTAVA MOBILNOG PLAĆANJA

Kada govorimo o tradicionalnim plaćanjima ona uključuju trgovca, posrednika, izdavača i potrošača, dok je kod mobilnog plaćanja postoje još dva dodatna sudionika koji su neizostavan dio ekosustava mobilnog plaćanja. Lanac vrijednosti mobilnog plaćanja uključuje više sudionika od tradicionalnih načina plaćanja i uvodi promjene. Lanac vrijednosti za mobilna plaćanja može se najbolje razumjeti ako se usporedi s uspostavljenim lancem vrijednosti plaćanja kreditnom karticom, [2].

4.1. Lanac vrijednosti ICT ekosustava

Ekosustav ICT tržišta mora se razvijati i prilagođavati zahtjeve za privatne subjekte, poslovne subjekte i vladajuća tijela. Svaki ekosustav u ICT okruženju funkcionira tako da svatko radi dio posla u kojem je „najbolji“ i na kraju se dijeli uspjeh ovisno o uključenosti sudionika u vrijednosni lanac. Svaki vrijednosni lanac ima svoju ponudu i potražnju (slika 13) te opis proizvoda, usluga i njihovih odnosa. Svaka karika lanca dodaje novu vrijednost prije predaje rezultata svoje aktivnosti sljedećoj karici lanca. Moguća su pokrivanja dijela vrijednosnog lanca (interni vrijednosni lanac) modifikacija i dorade vrijednosnog lanca novim sudionicima i novim poslovnim modelima kao što je slučaj kod ekosustava mobilnog plaćanja, [27].



Slika 13: Prikaz potražnje i ponude u ICT vrijednosnom lancu

Izvor: [27]

Usporedbom ICT vrijednosnog lanca s vrijednosnim lancem mobilnog plaćanja vidimo da su to dva slična ekosustava gdje je ekosustav mobilnog plaćanja podsustav ICT sustava te kao takav mora kroz svoj rad i funkcioniranje cijelog sustava imati sve sudionike ponude i potražnje navedene u ICT vrijednosnom lancu. Svaki sudionik može imati jednu ili više uloga unutar vrijednosnog lanca (mreža, poslužitelji, usluga, aplikacija, sadržaj), dok osnovne sudionike predstavljaju korisnici i davatelji sadržaja.

4.1.1. Korisnik

Nemoguće je zadovoljiti potrebe svakog pojedinca tako korisnike treba segmentirati odnosno grupirati osobe kako bi usluga ili sustav bio isplativ te pronaći ciljano osobe koje bi ponuđena usluga mogla zanimati. Segmentacija jest definiranje grupe korisnika sličnih karakteristika za koje je moguće kreirati različite usluge koje odgovaraju pojedinoj grupi. Mnoštvo načina segmentacije godine, spol, nacionalnost, zanimanje, prihodi, socijalni status, interesi. Cilj je definirati segmente koji se mogu jasno razlikovati od ostalih, a unutar kojih individualci dijele zajedničke karakteristike.

Postoje 3 dimenzije podataka o korisnicima:

- korisnik,
- korisničko ponašanje i
- korisnička vrijednost

Kada govorimo o podatcima o **korisniku** osnovno podatci koji se moraju saznati su identificirati osobu, saznati geografske podatke odnosno adresu osobe, čime se bavi te u kojem sektoru djelatnosti radi, kako bi pružatelj usluge imao okviran uvid u to kolika je platežna moć korisnika, detalje korisnikovog računa ako želi plaćati karticom ili nekim od navedenih načina mobilnog plaćanja, [27].

Što se tiče **korisničkog ponašanja** tu treba odrediti koliko često korisnik koristi ponuđenu uslugu i u kojim količinama, zatim povijest plaćanja i mobilnost prilikom korištenja ponuđene usluge. Kod korisničkog ponašanja bitno je znati i podatke o interakciji kao što su broj kontakata, vrijeme zadnjeg korištenja usluge i razne druge detalje kako bi se stvorila slika pojedinog korisnika, [27].

Zadnja dimenzija podataka o korisnicima jest **korisnička vrijednost.** Za pružatelja usluge vrijednost korisnika predstavlja njegovo zadovoljstvo ponuđenom uslugom. Također bitnu vrijednost čine prihodi korisnika te njegov trošak da se vidi koliko je korisnik spreman potrošiti za neku uslugu. Potrebno je ponuditi personaliziranu uslugu uz razumijevanje korisničkih potreba. I na kraju svakako identificirati najvrjednije korisnike koji čine potencijal te ih dodatno nagraditi ili smisliti način kako ih zadržati, [27].

Na temelju navedenog može se doći do zaključka da je korisnik potrošač usluga, aplikacija i pristupa mreži. Predstavlja organizaciju ili pojedinca (poslovni/privatni korisnik). Može biti i

pretplatnik odnosno korisnik koji je sklopio ugovor s davateljem usluga u svrhu korištenja usluga svaka fizička ili pravna osoba koja je sklopila ugovor s operatorom javno dostupnih elektroničkih komunikacijskih usluga o pružanju tih usluga.

4.1.2. Korisnički terminalni uređaji

Čine ga korisnička terminalna oprema, mrežna komunikacijska oprema i programska oprema. Kod ekosustava mobilnog plaćanja predstavlja najbitniji dio funkcioniranja cjelokupnog ekosustava jer je mobilni terminalni uređaj u središtu poslovnog modela te se oko njega odvijaju svi procesi koji su važni za ekosustav mobilnog plaćanja.

Najkorišteniji terminalni uređaj o kojem se najviše i govori u radu jest mobilni uređaj**. Mobilni telefon** prijenosni je elektronički uređaj za komunikaciju. Glavna komunikacijska funkcija je glasovna komunikacija, no u novije vrijeme dodane su funkcije kao: kratke tekstualne poruke (SMS) te kratke slikovne poruke (MMS). Mobilni telefoni se razlikuju od prijenosnih telefona po većem dometu i nisu vezani uz jednu baznu stanicu. Za uspostavljanje govorne veze s drugim mobitelom koristi se bežično spajanje na mrežu baznih stanica. Pametni mobiteli imaju funkcionalnosti i aplikacije za primanje elektroničke pošte putem Interneta, registraciju kontakata, kalkulator, sat, alarm, igre, programe za reprodukciju glazbe i videa, *Instant Messaging* i razne druge aplikacijske usluge od kojih su svakako i aplikacije mobilnog plaćanja.

S obzirom na to da se u radu govori o mobilnom plaćanju treba napomenuti da mobilno plaćanje nije doslovno vezano samo za mobilni terminalni uređaj.

Plaćanje **pametnim satom** (slika 14) iako još skroz nije razvijeno u hrvatskoj moguće je i koristi se u nekim državama. Ako se na sat doda kartica za plaćanje korisniku neće biti potreban mobilni telefon za plaćanje. Plaćanje u trgovini pomoću pametnog sata sastoji se od sljedećih koraka:

1. na satu se otvori aplikacija Google Pay, Samsung Pay ili Android Pay
2. korisnik prisloniti sat na čitač za beskontaktno plaćanje dok ne začuje zvuk ili osjeti vibriranje sata.
3. Ako se prikaže uputa da to učini, korisnik odabere "kreditna", neovisno o vrsti kartice.
4. Tijekom transakcija s debitnom karticom možda će trebati unijeti PIN kod. Korisnik koristi PIN kod koji mu je dodijelila banka.

S obzirom na raznolikost terminalnih uređaja, izdvojit će se još par najkorištenijih koji se koriste za usluge mobilnog plaćanja. Ali općenito svaki pametni uređaj koji ima mogućnost

pohranjivanja podataka o kartici i pristup Internetu trebao bi moći ostvarivati usluge mobilnog plaćanja.

Od terminalnih uređaja kojima se može još ostvariti mobilno plaćanje svakako treba izdvojiti **tablet** koji ako ima mogućnost dodavanja SIM kartice posjeduje sve funkcionalnosti kao i mobilni uređaj. Tako da se plaćanje provodi slično kao na mobilnom uređaju, uz napomenu da svakako tablet mora posjedovati neki od načina mobilnog plaćanja koji su navedeni kroz rad. Također je neophodno da posjeduje neku tehnologiju NFC, HCE, Bluetooth ili druge koje su ranije objašnjene u radu.

Terminal za plaćanje POS uređaj je koji se koristi s platnim karticama za obavljanje elektroničkih prijenosa sredstava . Terminal se obično sastoji od sigurne tipkovnice za unos PIN-a, zaslona, sredstva za prikupljanje podataka s platnih kartica i mrežne veze za pristup mreža plaćanja za autorizaciju. Terminal za plaćanje omogućava trgovcu da zabilježi potrebne podatke o kreditnoj i debitnoj kartici i da te podatke proslijedi pružatelju usluga ili banci trgovačkih usluga radi autorizacije i, na kraju, da prenese sredstva trgovcu. Terminal omogućava trgovcu ili njegovom klijentu da prevuče prstom, umetne ili drži karticu u blizini uređaja za snimanje podataka. Oni su često povezani sa sustavima prodaje, tako da se iznosi plaćanja i potvrda plaćanja mogu automatski prenijeti u sustav upravljanja maloprodajom trgovaca.

Slika 14: Primjer plaćanja pametnim satom na POS terminalu za plaćanje

Izvor: [28]

4.1.3. Mreža

Kada govorimo o prijenosu podataka s uređaja do POS uređaja potrebno je imati neku lokalnu mrežu kako bi se raj prijenos podataka ostvario na brzinu i uz maksimalnu sigurnost i zaštitu podataka. Kad govorimo o lokalnom prijenosu podataka s uređaja na POS uređaj za plaćanje najkorištenija tehnologija, a u ovom slučaju jest NFC, iako su ranije u trećem poglavlju rada spomenute razne tehnologije pomoću kojih bi se prijenos podataka lokalno mogao ostvariti sigurno i na brzinu, NFC je najkorištenije i najbolje rješenje za prijenos podataka lokalno.

Osim lokalnog prijenosa podataka s korisnikovog uređaja na POS uređaj za plaćanje podatke o plaćanju i samu novčanu transakciju je potrebno prenijeti na siguran način od POS uređaja trgovca do ostalih sudionika vrijednosnog lanca ekosustava mobilnog plaćanja. Takva ICT mreža je cjelovita usluga koja omogućuje realizaciju lokalne mreže na lokaciji korisnika, a koja je bazirana na žičnim i bežičnim tehnologijama.

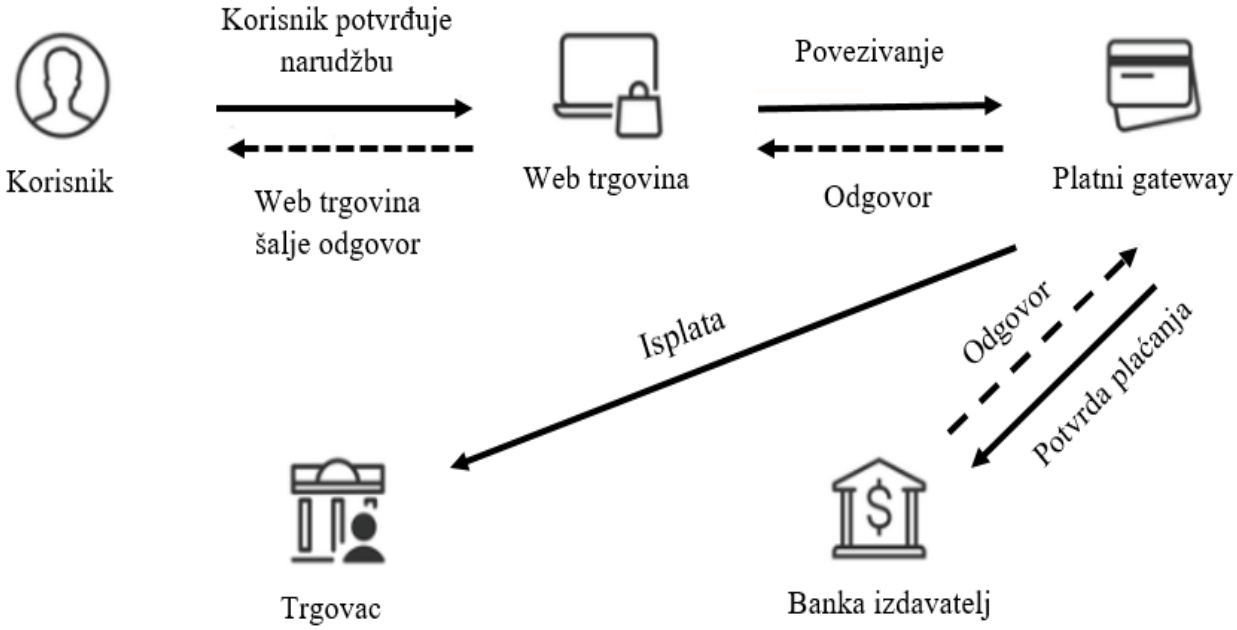
Za ostvarivanje usluga mobilnog plaćanja mogu se koristiti različite mreže. Osnovna podjela mreža pomoću kojih se ostvaruje prijenos novčanih transakcija od POS uređaja do ostalih sudionika ekosustava jest na nepokretne i pokretne mreže. Nepokretna mreža jest javno dostupna telefonska usluga u nepokretnoj elektroničkoj komunikacijskoj mreži gdje postoji 50-ak operatora u Republici Hrvatskoj (HAKOM). Korisnici mogu pomoću LAN, MAN, WAN mreža pristupiti Internetu i obavljati novčane transakcije koristeći usluge mobilnog plaćanja.

Pokretna mreža jest javno dostupna telefonska usluga u pokretnoj elektroničkoj komunikacijskoj mreži. Usluge u pokretnoj telefoniji obuhvaćaju pružanje usluga pokretnih telekomunikacija putem GSM mreže. Globalni sustav za mobitele ili GSM najzaposleniji je mobilni standard na svijetu. Ostale tehnologije uključene u GSM standard su GPRS i EDGE, koji nude brži prijenos podataka u 2G mrežama. HSDPA, ili brzi pristup paketnoj brzini je 2G GSM mreža. CDMA višestruki pristup Code Division ili CDMA novija je tehnologija i nudi veće mogućnosti prijenosa podataka. Long Term Evolution ili LTE, je sljedeća generacija stanične tehnologije poznata kao (4G LTE). Sve navedene tehnologije koriste se za ostvarivanje komunikacije u pokretnoj mreži pomoću mobilnog uređaja.

4.1.4. Poslužitelj

Raspolaže računalnim i komunikacijskim sustavima s odgovarajućim memorijskim kapacitetom i kapacitetom obrade za potrebe svojih korisnika. Poslužitelj kao bitan dio ICT ekosustava pruža informacijsko komunikacijske usluge korisnicima putem telekomunikacijskih mreža (fiksna i mobilna mreža) npr. glasovna i video telefonija i slično. Glavne odgovornosti pružatelja usluga su: upravljanje profilima korisnika, pribavljanje i zadržavanje pretplatnika, pružanje usluga sigurnosti, tarifiranje i naplata za korištenje usluga. Kod ekosustava mobilnog plaćanja poslove poslužitelja ICT ekosustava obavljaju banka stjecatelj i banka izdavatelj te operator mobilne mreže, [27].

Poslužiteljev pristup ovisi o tehnologiji koja se koristi za integriranje plaćanja kreditnom ili debitnom karticom u mobilne aplikacije i na web stranice. To je među najboljim postupcima za obradu plaćanja putem Interneta. Pristupnik plaćanja ili poslužitelj je odgovoran za sigurno prikupljanje podataka o klijentima na prednjem dijelu aplikacije i potom slanje banci koja ga prima ili platnom procesu kako bi obavio transakciju.



Slika 15: Primjer funkcioniranja gateway poslužitelja

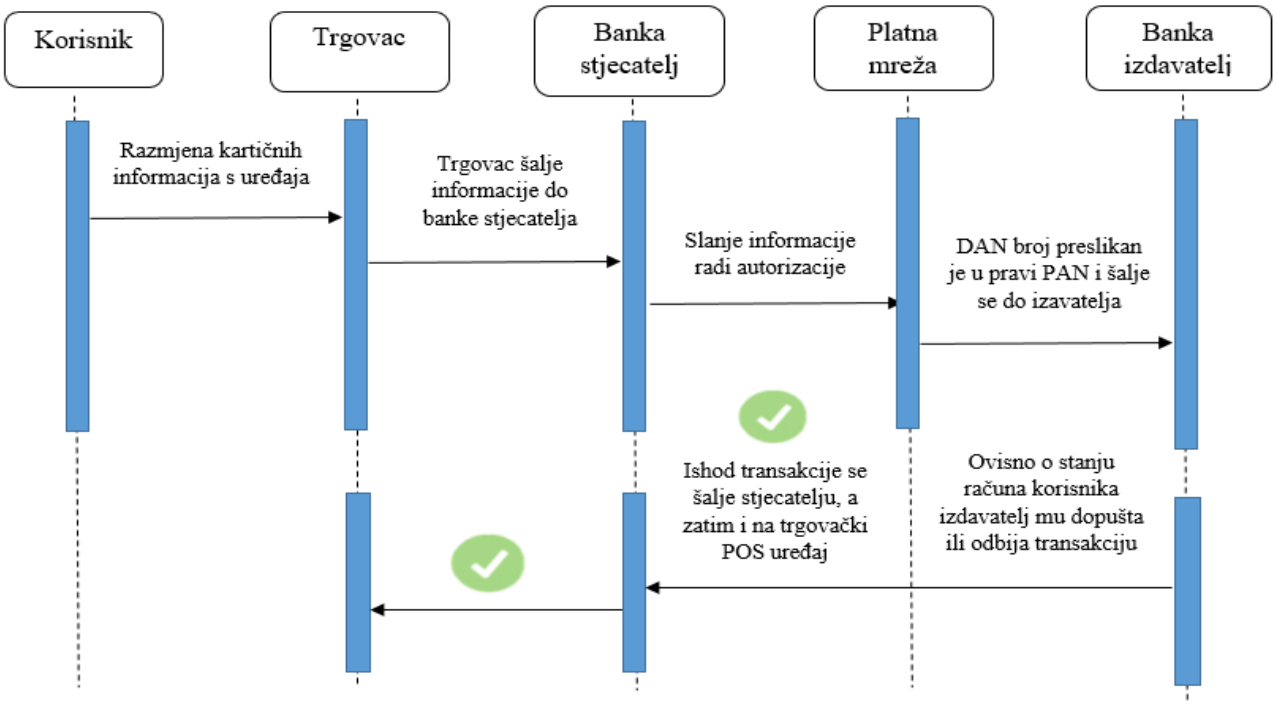
Izvor: [26]

Kada korisnik potvrdi narudžbu web trgovina korisniku šalje odgovor o potvrdi primitka narudžbe, zatim se Web trgovina povezuje s poslužiteljem (slika 15) odnosno u ovom slučaju platnim gateway-om koji šalje odgovor da je komunikacija ostvarena. Ako korisnik ima dovoljno sredstava na računu vrši se isplata prema trgovcu koji je postavio proizvod ili uslugu na Web trgovinu. Kako bi sve prošlo uz sigurnost i zaštitu informacija koje se prijenose, kontaktira se banka izdavatelj (koja je ovdje također u ulozi poslužitelja) kojoj se također šalje potvrda o plaćanju. Nakon čega banka šalje odgovor o mogućnosti ili ne mogućnosti plaćanja. Ako je odgovor pozitivan vrši se navedena isplata.

4.1.5. Usluge i aplikacije

Davatelj aplikacijskih usluga brine se za upravljanje ponudom aplikacija prema krajnjem korisniku te prodaje korištenje aplikacija na komercijalnim principima. Kako bi se najbolje opisao način rada aplikacijskih rješenja za ekosustav mobilnog plaćanja u nastavku rada nabrojat će se ekosustav 3 najkorištenije aplikacije mobilnog plaćanja Apple Pay, Samsung Pay i Android Pay.

Apple Pay usluga mobilnog plaćanja i digitalni novčanik tvrtke Apple koja omogućuje plaćanje osobno, putem iOS aplikacija i na webu. Može se koristiti na iPhoneu, Apple Watchu, iPadu i Macu. Digitalizira i može zamijeniti čip kreditne ili debitne kartice i transakciju s PIN-om na terminalu prodajnog mjesta. Apple Pay surađuje s bilo kojim trgovcem koja prihvaća beskontaktno plaćanje. Za zaštitu podataka Apple Pay koristi *Touch ID, Face ID,* PIN ili lozinke. Uređaji bežično komuniciraju sa sustavima prodajnih mjesta koristeći NFC. Kada se Apple Pay-u doda nova platna kartica (tj. kreditna ili debitna) proces koji se događa u pozadini bit će objašnjeni kroz dijagram, [20].



Slika 16: Sekvencijalni dijagram Apple Pay platnog procesa

Izvor: [20]

Kada govorimo o ekosustavu aplikacije Apple Pay čine ga: korisnici koji posjeduju iPhone ili neki od Apple uređaja, zatim TSP (TSP je sustav unutar ekosustava mobilnog plaćanja koji je u mogućnosti pružiti registriranim podnositeljima zahtjeva za tokenima, na primjer trgovcima koji posjeduju vjerodajnice kartice vrijednosne tokene), koji se brine za zaštitu i sigurnost korisnikovih informacija koji generira dinamički kriptogram što je kombinacija tokena plaćanja, iznosa transakcije i brojača transakcije zajedno s ključem plaćanja tokena odnosno javnim ključem plaćanja tokena TSP.

Sljedeći sudionik u ekosustavu Apple Pay-a jest banka stjecatelj koja je na strani trgovca koji posjeduje POS uređaj za komunikaciju s Apple Pay aplikacijom i šalje zahtjev koji se prosljeđuje do nekih od platnih mreža *Visa* ili *MasterCard* i druge. Sljedeći sudionik jest ranije spomenuta mreža plaćanja koja utvrđuje da je zahtjev koji je pristigao u obliku tokena DAN (broj koji zamjenjuje PAN), a ne pravi PAN, te na temelju toga donosi token za plaćanje do TSP-a za dobivanje povezanog PAN-a. Zahtjev potvrđuje dešifriranjem dinamičkog kriptograma (koji sadrži javni ključ plaćanja-token) pomoću privatnog ključa *Payment-Token*. Jednom kada je zahtjev potvrđen, TSP traži PAN koji se povezuje s tokenom plaćanja unutar trezora tokena i

vraća stvarnim PAN u platnu mrežu. Platna mreža nakon što je primila pravi PAN prosljeđuje ga do banke izdavatelja. Banka izdavatelja sljedeći je sudionik u ekosustavu Apple Pay-a koja provjerava stanje računa klijenta u odnosu na iznos transakcije i ovlašćuje traženi zahtjev, zatim Banka izdavatelj vraća odgovor autorizacije na platnu mrežu što se zauzvrat vraća natrag banci stjecatelja (trgovca) , koja ga zauzvrat vraća na POS terminal, a transakcija se odobrava na POS zatim POS dalje to prenosi na iPhone putem NFC tehnologije. Na kraju se na telefonu dobiva zelenu potvrdu da je transakcija odobrena (Slika 16) te se tako završava ciklus plaćanja putem Apple Pay aplikacije, [20].

Samsung Pay je usluga mobilnog plaćanja i digitalnog novčanika koja korisnicima omogućuje plaćanja putem kompatibilnih telefona i drugih uređaja proizvedenih od Samsung-a. Usluga podržava beskontaktno plaćanje korištenjem NFC tehnologije, ali također podržava terminale za plaćanje podataka magnetske trake koje mu omogućuje MST tehnologija koja se emitira prelaskom trajne magnetske trake pored čitača stvaranjem magnetskog polja u blizini POS uređaja što je objašnjeno prethodno u radu. Kad se drži telefon uz bilo koji terminal on emitira signal koji simulira magnetsku traku na kartici.

Samsung pay aplikacija može se koristiti za; pametne telefone i nosive uređaje te omogućuje plaćanje robe i usluga blizu beskontaktnog platnog terminala POS) pomoću Samsung uređaja ili autorizacijom plaćanja putem Interneta bez korištenja gotovine ili kreditnih kartica. Zahvaljujući korištenju NFC i MST tehnologije Samsung Pay široko je prihvaćen. Zbog korištenja dvije tehnologije Samsung Pay se može koristiti na gotovo bilo kojem mjestu plaćanja te mu to daje prednost u odnosno na konkurentne mobilne novčanike, [21].

S obzirom na to da je ekosustav mobilnog plaćanja ranije objašnjen kod Apple Pay-a, a nema mnogo razlike u odnosu na Samsung Pay ovdje će se pisati o sigurnosti, jer je to jedan od najbitnijih faktora u procesima plaćanja te često predstavlja najveći problem jer se korisnicima treba na što vjerniji način prikazati kako je neka aplikacija, uređaj ili način plaćanja siguran jer se sve što se tiče sigurnosti događa u pozadini.

Kada korisnik doda svoju platnu karticu na Samsung Pay informacije se šifriraju i šalju na Samsung poslužitelje, a u konačnici na platnu mrežu izdavača kartice (tj. *Visa, MasterCard* ili *American Express*) radi odobrenja. Izdavač kartice može zatražiti jednokratnu lozinku kako bi potvrdio da je korisnik stvarni vlasnik kartice. Ako se kartica ikad izgubi ili ukrade, to što korisnik već ranije posjeduje lozinku za Samsung Pay spriječit će lažno dodavanje kartice na

Samsung Pay. Kada se izvrši plaćanje korisnik potvrđuje svoj identitet pomoću otiska prsta ili PIN-a. Trgovac će dobiti samo token, a podaci o plaćanju bit će zaštićeni. Token će biti poslan mreži plaćanja gdje će se dešifrirati i provjeriti u skladu s podacima pohranjenim u sigurnom trezoru na internim mrežama. Nakon ovjere plaćanje će biti odobreno i poslano natrag trgovcu. Podatke o transakciji imaju samo platna mreža i korisnikova banka, [21].

Nakon nadogradnje upravljačkog softvera korisnik može preuzeti aplikaciju Samsung Pay i spremiti u aplikaciji svoje podatke o kreditnoj kartici i debitnoj kartici. Sljedeći put kada treba izvršiti plaćanje to može učiniti pomoću aplikacije Samsung Pay koristeći samo neki od Samsung uređaja koji podržavaju Samsung Pay aplikaciju. Proces korištenja usluge Samsung Pay koji zamjenjuje fizičku karticu objašnjen je u 3 jednostavna koraka. Korisnik Samsung uređaja koristi svoj Samsung galaxy S7 uređaj (slika 17) za ulazak u aplikaciju Samsung Pay, [7];

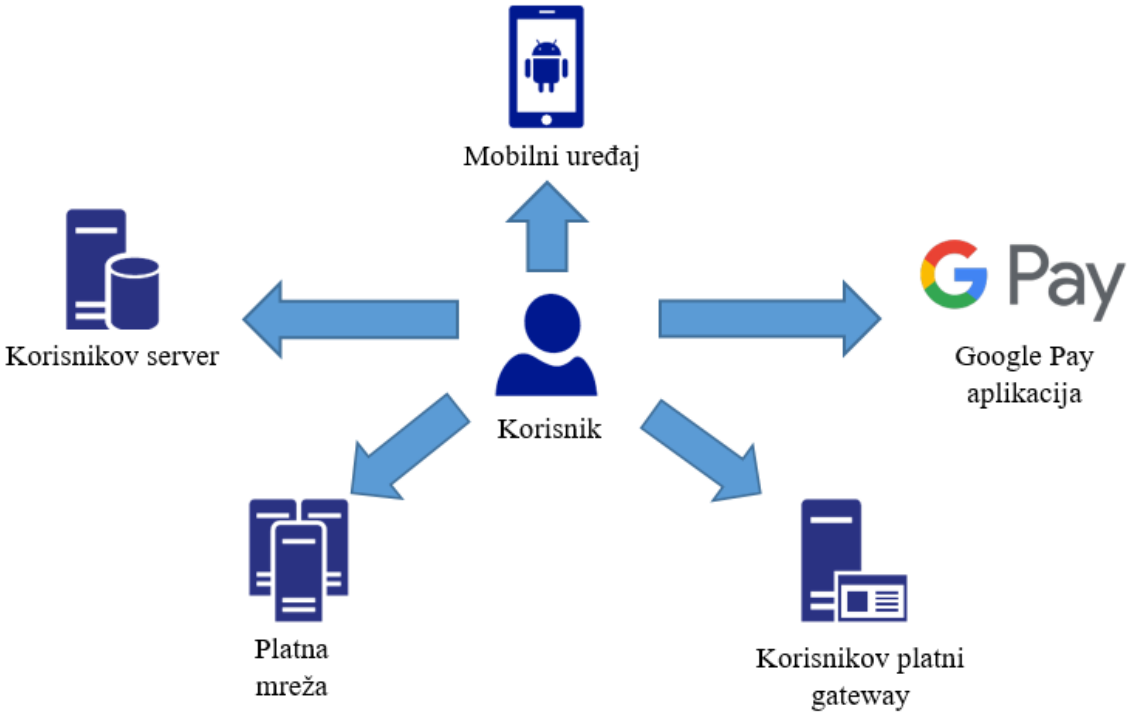
- korisnik povuče prstom prema gore na zaslonu svog uređaja te mu se pojavljuje kartica,
- proces autentifikacije se vrši s PIN-om ili kako je prikazano na slici otiskom prsta, nakon što je autentifikacija odobrena na uređaju se prikazuje virtualna kartica koja izgleda kao prava kartica sa svim svojim karakteristikama i
- zadnji korak se sastoji od toga da se mobilni uređaj primakne dovoljno blizu POS uređaju kako bi se svi podatci mogli očitati pomoću NFC ili MST tehnologije koje su prethodno objašnjene.

Slika 17: Prikaz korištenja Samsung Pay aplikacije u 3 jednostavna koraka

Izvor: [21]

Google Pay je platforma za digitalni novčanik i mrežni platni sustav koji je Google razvio za korištenje putem aplikacija i kupovine robe i usluga na mobilnom uređaju, omogućavajući korisnicima plaćanje putem Android telefona, tableta ili pametnih satova. Od 8. siječnja 2018. stari Android Pay i Google novčanik ujedinili su se u jedinstveni sustav plaćanja koji se zove Google Pay. Android Pay preimenovan je u naziv Google Pay. Google Pay prihvaća značajke i Android Paya i Google novčanika putem internetskih prodavaonica i usluga plaćanja putem Interneta. Google Pay aplikacija nudi standardnu funkcionalnost kao i svaki digitalni novčanik dodavanje kreditnih kartica, kartica vjernosti, platnih kartica itd. Zajedno s funkcijama koje pokreće Google.

Kako Google Pay radi i što se sve događa u pozadini prikazano je kroz sudionike te dalje objašnjeno kroz korake, prikazano je što se sve događa prilikom korištenja Google Pay-a kao načina mobilnog plaćanja i nabrojani su svi sudionici uključenih (slika 18) u ekosustavu Google Pay aplikacije, [23].



Slika 18: Prikaz sudionika Google Pay ekosustava

Izvor: [23]

Čitav ekosustav upotpunjava Googleovu viziju zadovoljavanja potreba i praćenjem svih online aktivnosti pojedinca te tako uz razna dopuštenja dobiva hrpu informacija o pojedincu, o njegovim potrebama, navikama, željama i svemu što pretražuje na internetu. Na temelju toga Google prilagođava ponudu usluge povezujući; karte, pretraživanje, recenzije i platne procese pojedinca kako bi mu pružio preciznu verziju podataka usmjerenu na mjesto ili web aplikaciju kako bi i dalje trošio i koristio njihovu uslugu plaćanja. Kako to izgleda kroz korake od trenutka kada korisnik odluči nešto platiti pa do potvrde da je u mogućnosti platiti traženi proizvod ili uslugu objašnjeno je kroz sljedeće korake;

1. **korak**: korisnik odlučuje platiti pomoću Google Paya;

   Korak 1.1 : Skripta uređaja pokreće API (*Google API* su skup aplikacijskih programskih sučelja API (eng. *Application Programming Interface)* koje je razvio Google i omogućuju komunikaciju s Googleovim uslugama te njihovu integraciju u druge usluge) poziv na uslugu Google Pay radi identifikacije zahtjeva za plaćanje. Uzimajući kartice i njihove identifikatore

   Korak 1.2 : Zahtjevi skripte za adresu, iznos plaćanja, podatke o otpremi itd. Potrebni za dovršavanje transakcije za e-trgovinu ovdje se određuje koji su zahtjevi za unos i dostupne opcije isporuke podataka.

2. **korak**: korisnik potvrđuje plaćanje pomoću PIN-a. Na Google Pay uslugu se postavlja zahtjev za preuzimanje detalja kartice s obzirom na poslane identifikatore kartice.
3. **korak**: ako su podaci o kartici tokenizirani (što je slučaj kod većine pružatelja usluga), Google Pay službe postavljaju zahtjev da dobiju token za poslani identifikator.
4. **korak:** platna mreža vraća odgovarajući token i kriptogram na Google Pay uslugu.
5. **korak:** Google stvara šifrirane podatke o plaćanju pomoću ključa specifičnog za pristup koji se isporučuje u zahtjevu za novčanik i uključuje ih u odgovor na Google API.
6. **korak:** Skripta uređaja upućuje poziv poslužitelju sa šifriranim podatcima iz odgovora Google API-ja i objektom narudžbe koji sadrži podatke o proizvodu.

7. **korak:** Zahtjev od poslužitelja do poslužitelja gdje se pokreće plaćanje. Nakon toga poslužitelj priprema informacije o odgovoru s Google Paya za slanje na gateway uslugu. Gateway (banka koja obavlja dolazne uplate sa stranom s kojom korisnik ima bankarski odnos) kupcu šalje zahtjev za autorizacijom. Kupac obrađuje zahtjev s *gatewaya* i stvara zahtjev za autorizaciju mreže plaćanja. Mreža za plaćanje obrađuje zahtjev kupca i stvara zahtjev za izdavanje autorizacije izdavatelja (izdavatelj je banka koja je kupcu izdala kreditnu karticu, ranije objašnjeno u radu). Izdavatelj pregledava podatke o plaćanju i vraća odobrenu ili odbijenu poruku autorizacije na platnu mrežu. Nakon toga mreža za plaćanja vraća odgovor autorizacije kupcu, a kupac vraća odgovor autorizacije na gateway.
8. **korak:** Nakon što se sve obavi u prethodnom koraku, cijeli odgovor se vraća na korisnikov poslužitelj, a u slučaju da je sve prošlo uredno stvara se narudžba.
9. **korak:** odgovor se vraća na uređaj. U slučaju uspjeha korisnik se upućuje na stranicu potvrde narudžbe, dok se u slučaju neuspjeha prikazuje poruka o pogrešci.

4.1.6. Sadržaj

Sadržaj unutar aplikacije može se slobodno staviti kao primarno sredstvo za preuzimanje ili kupnju pojedinih aplikacija. Upravo zbog sadržaja koji se nude unutar samih aplikacije se i same aplikacije preuzimaju. Postoji nekoliko sudionika kada je sadržaj u pitanju. Dakle postoji vlasnika sadržaja koji raspolaže informacijom u izvornom obliku te on kao takav ima komercijalna i autorska prava, ne mora nužno značiti da je ujedno i davatelj sadržaja. S druge strane imamo davatelja sadržaja koji je ujedno i vlasnik istoga.

Davatelji sadržaja mogu pomoći aplikaciji u upravljanju pristupom pohranjenim podacima, pohranjenim u drugim aplikacijama i na način dijeljenja podataka s drugim aplikacijama. Oni obuhvaćaju podatke i pružaju mehanizme za definiranje sigurnosti podataka. Davatelji sadržaja su standardno sučelje koje povezuje podatke u jednom procesu s kodom koji se izvodi u drugom procesu. Primjena davatelja sadržaja ima brojne prednosti.

Najvažnije je da se usklade davatelji sadržaja kako bi dopuštali drugim aplikacijama siguran pristup i izmjenu podataka o njihovim aplikacijama. Zatim postoji još i veletrgovac sadržajem koji otkupljuje sadržaje od vlasnika ili omogućavatelja te ih nudi na tržištu, omogućavatelj sadržaja koji priprema izvornu informaciju za daljnje oblikovanje, objavljivanje, obradu, pohranu i pretraživanje. Dok sakupljač sadržaja i aplikacija osigurava krajnjem korisniku pristup

do brojnih usluga s dodanom vrijednošću, moguće je kombinirati tu ulogu s ulogom mrežnoga operatora ili s onom isporučitelja aplikacija, [27].

Sadržaj predstavlja informaciju koja se prenosi i zbog kojeg svi uključeni sudionici ekosustava i obavljaju svoje poslove kako bi sadržaj stigao u izvornom obliku od jedne do druge točke. Sadržaji u ICT ekosustavu može biti (npr. streaming, spremanje sadržaja), interaktivne usluge (igranje, prisutnost), osobne usluge (bankarstvo), komunikacija (e-mail), m-trgovina (m-commerce) i razni drugi. Dok kod ekosustava mobilnog plaćanja predstavlja informacije o transakcijama odnosno sve ono što se prenosi uz novčanu transakciju kako bi se sve obavilo bez ometanja i poteškoća uz maksimalnu zaštitu informacija koje se prijenose.

Analizom cijelog vrijednosnog lanca ICT ekosustava i svih njegovih sudionika napravljena je podloga kako bi se u sljedećem poglavlju jasno opisali sudionici poslovnog modela ekosustava mobilnog plaćanja, s obzirom na to da je ekosustav mobilnog plaćanja također jedan ICT ekosustav tako da su svi sudionici ICT ekosustava također sudionici ekosustava mobilnog plaćanja.

4.2. Sudionici poslovnog modela ekosustava mobilnog plaćanja

S obzirom na to da je u prethodnom poglavlju opisan ekosustav ICT tržišta može se zaključiti kako je to složen sustav te kako takvih sustava ima miliju zbog razvoja Interneta, usluga i tehnologija. Jedan od značajnijih ekosustava u IK domeni jest ekosustav mobilnog plaćanja. S obzirom da su ranije opisani svi bitni sudionici ICT ekosustava te što rade i koja im je glavna zadaća i smisao egzistencije, u ovom poglavlju će se spomenuti navedeni sudionici ICT ekosustava koji su uključeni u ekosustav mobilnog plaćanja. Spomenuti će se svi sudionici vrijednosnog lanca ICT ekosustava te će se provesti detaljna analiza njihove uloge u ekosustavu mobilnog plaćanja.

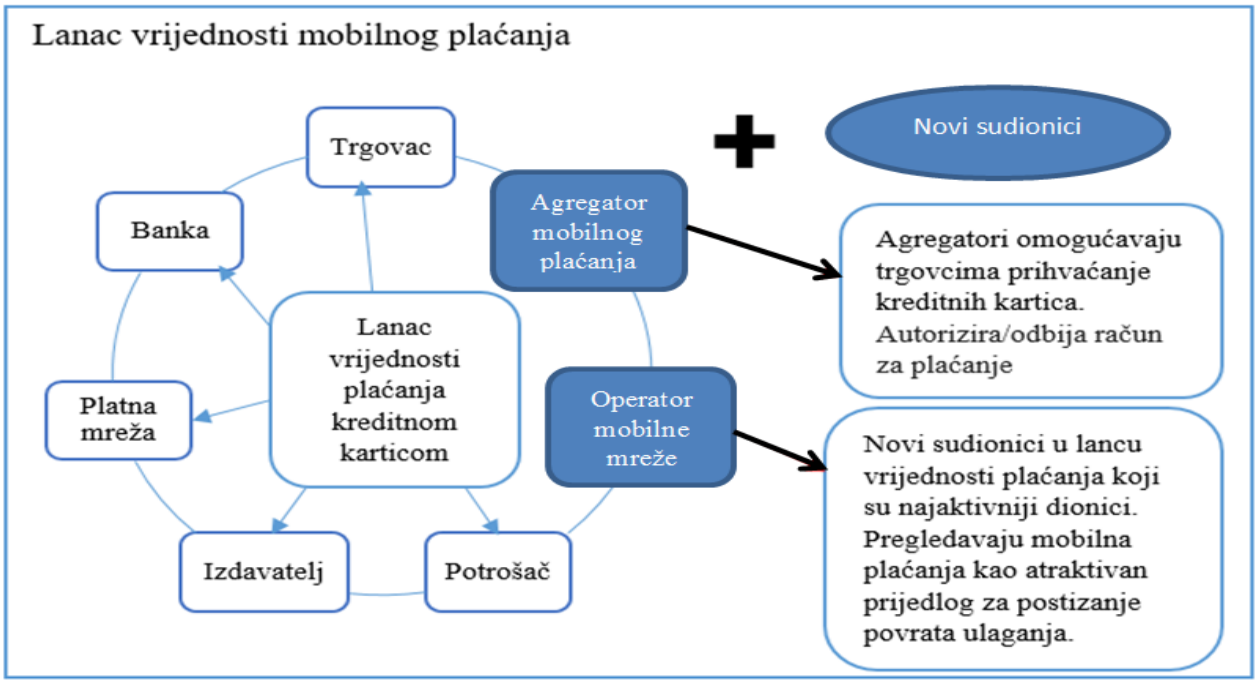
Poslovni model mobilnog plaćanja ima slične dionike kao kreditna kartica. Uvođenje plaćanja mobilnim kanalom privukla su mnogo novih sudionika mobilnog ekosustava. Većina tih sudionika potječe iz sektora mobilne komunikacije. S obzirom na to da kreditna kartica ima od prije uspostavljeni ekosustav plaćanja što je navedeno (tablica 1), ekosustav mobilnog plaćanja dodaje 2 nova sudionika na postojeći ekosustav. To su operator mobilne mreže te agregator mobilnog plaćanja koji djeluje kao posrednik, ta dva sudionika te ostali sudionici u ekosustavu mobilnog plaćanja bit će opisani dalje u tekstu, [2].

Tablica 1: Prikaz sudionika lanca vrijednosti plaćanja kreditnom karticom

Kupac	Trgovac	Banka	Platna mreža	Izdavatelj
Kupnja robe ili usluge od trgovaca. Omogućuje trgovcima plaćanje informacija o računu.	Vlasnik/zakup softver/hardver za ovjeru i procesno plaćanje informacije o računu. Stvara račun za transakciju i šalje ga banci.	Trgovačka banka. Plaćanje kontakata i mreža za provjeru na sredstva za naplatu. Pruža bankarske usluge za trgovca.	Posrednik između banke i izdavatelja ostvaruje komunikaciju između banaka.	Potrošačka banka koja daje kredit ili zaduženje potrošaču. Ovlašćuje ili odbije plaćanje računa izdanog od trgovca. Šalje uplatu kupcu ako kupac ima odobrena sredstva.

Izvor: [6]

Svaki ICT (eng. *Information and Communication Technology*) sustav pa tako i ekosustav mobilnog plaćanja jest samoorganizirajući sustav tržišta, mreža, usluga, aplikacija i sadržaja te vladajućih, pravnih i regulatornih tijela. Lanac vrijednosti mobilnog plaćanja (slika 19) za razliku od lanca vrijednosti plaćanja kreditnom karticom dodaje još operatora mobilne mreže i agregatora mobilnog plaćanja kao nove sudionike u ekosustavu.



Slika 19: Lanac vrijednosti mobilnog plaćanja

Izvor: [2]

4.2.1. Operatori mobilne mreže

Novi su sudionici u lancu vrijednosti plaćanja i oni su najaktivniji sudionici. U usporedbi s ICT vrijednosnim lancem operator mobilne mreže jest na strani ponude. Jer pruža informacijsko komunikacijske usluge korisnicima putem telekomunikacijskih mreža (fiksna i mobilna mreža) – npr. glasovna i video telefonija i slično, druge glavne odgovornosti su: upravljanje profilima korisnika, pribavljanje i zadržavanje pretplatnika, pružanje usluga sigurnosti, tarifiranje i naplata za korištenje usluga, [27].

Glavna zadaća mobilnog operatora u ekosustavu mobilnog plaćanja jest direktna naplata s korisnikovog računa za mobilnu ili fiksnu mrežu jer tako olakšava korisnicima naplatu i sve komplikacije vezane za platne transakcije. Naplata putem operatora daljinski je način plaćanja koji korisnicima omogućuje plaćanje internetske robe, proizvoda, podrške, usluga i sadržaja putem svojih mobilnih uređaja (mobilnih telefona, tableta i pametnih televizora). Ovakav način plaćanja omogućava korisnicima da koriste opciju plaćanja mobilnim uređajem, a financijska sredstva im se izravno naplate s mobilnog računa.

Metoda izravne naplate za mobilne uređaje ne zahtijeva postupak registracije, kratke brojeve ili duge obrasce. Umjesto toga pretplatnici mobilne mreže mogu kliknuti i kupiti željeni proizvod ili uslugu u nekoliko sekundi, jer će se sadržaj koji kupuju sigurno teretiti od njihovog aktivnog

računa za mobilne telefone. Naplata putem mobilnog operatora osim brzine i sigurnosti plaćanja vrlo je fleksibilna. S obzirom na to da su visoke stope isplate, ovaj način mobilnog plaćanja u ekosustavu mobilnog plaćanja se smatra preporučljivom metodom za mobilno plaćanje. Transakcijski troškovi svode se na minimum i nema dodatnih troškova niti skrivenih naknada uključenih u ovaj postupak plaćanja.

Najbolji dio ove vrste plaćanja je taj što je primjenjiv ne samo na korisnike pametnih telefona, već i na sve ostale korisnike telefona. Potrošačima je relativno lako vjerovati ovom načinu plaćanja jer se sva njihova plaćanja obrađuju preko njihovih telekom operatora koji ima svoj ekosustav koji automatski obavlja sve komplikacije vezane za autorizaciju, sigurnost, zaštitu transakcija i ostale radnje potrebne za sigurno mobilno poslovanje, Na tržištima u nastajanju izravno je naplata putem mobilnog operatera jedini način da korisnici kupuju mrežni sadržaj i usluge. Trgovci digitalnim sadržajem i fizičkim uslugama sve se više oslanjaju na naplatu putem mobilnog operatera jer se na tim tržištima nalazi sve veći broj njihovih korisnika, [2].

Slika 20: Prikaz uključivanja mobilnog operatora u lanac vrijednosti mobilnog plaćanja

Izvor: [2]

Kao što je prikazano (slika 20) potrošač koji je prethodno sklopio ugovor s mrežnim operatorom kupuje online knjigu od davatelja te usluge, nakon toga se vrši razmjena informacija odnosno naplata između davatelja usluge i mobilnog operatora, nakon čega mobilni operator obavještava kupca da može kupiti online knjigu i šalje mu potvrdu za to, a potrošaču se oduzimaju sredstva s računa u iznosu online knjige te mu se izdaje digitalni račun. Svi navedeni koraci se odvijaju u nekoliko klikova i u nekoliko minuta, s obzirom na to da su poslovi autorizacije i sigurnosti već ranije riješeni prilikom sklapanja ugovora s mobilnim operatorom tako se ubrzava proces naplate usluge kao i proces plaćanja usluge, što za krajnji rezultat daje zadovoljstvo potrošača, davatelja usluge i mobilnog operatora.

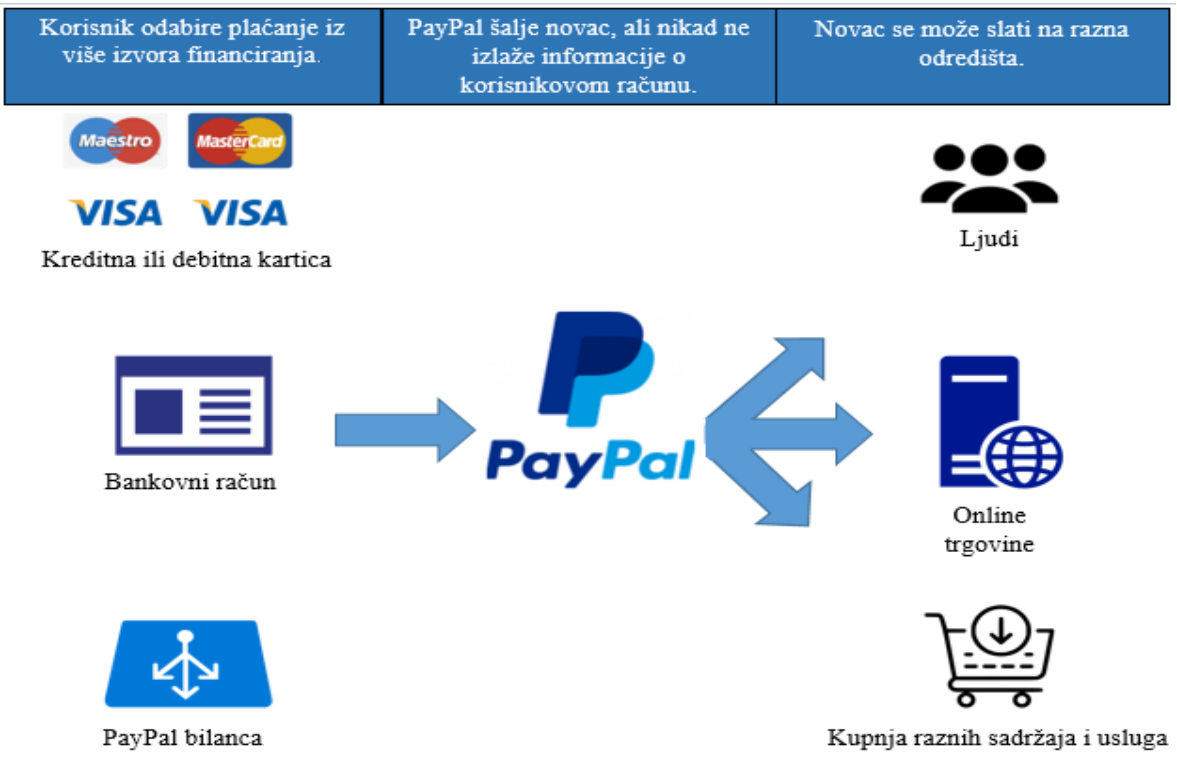
4.2.2. Financijske institucije (banke)

Kao jedan od bitnih dijelova u ekosustavu mobilnog plaćanja imaju dokazanu stručnost u upravljanju plaćanjima na siguran način, a kao sudionik u vrijednosnom lancu ICT tržišta banke mogu djelovati kao davatelj aplikacije za mobilno plaćanje. U ekosustavu za mobilni platni promet banke su u snažnom položaju zahvaljujući ključnim odnosima s trgovcima i kupcima, upravljanju rizikom i potrebnom infrastrukturom. Banke moraju osigurati pouzdanost platnih sustava i umanjiti šanse za prijevarom. Posjeduju resurse na 3 razine; to su ljudski, nematerijalni i opipljivi za mobilna plaćanja. Ljudski resursi su ljudi s kojima treba stvoriti vrijednost opipljivih i nematerijalnih resursa. Nematerijalni resursi u mobilnom plaćanju uključuju patente, marke i bankarsku licencu. Materijalni resursi uključuju dogovorenu uslugu i platnu infrastrukturu. Banke se suočavaju s jasnom prijetnjom ograničavanja rada s obzirom na sve veći napredak mobilnog plaćanja. To znači da su eliminirani kao financijski posrednici, čime gube privilegirani i izravni odnos kojeg su gradili sa svojim klijentima. U međuvremenu mobilne aplikacije za plaćanje preuzele su kontrolu nad cijelim procesom i nude različite usluge bez ikakve bankarske intervencije uključujući osnovne bankarske usluge poput provjere računa i aktiviranja štednih računa. S obzirom na navedeno banke se okreću novim rješenjima te se vrlo aktivno uključuju u mobilno bankarstvo kako bi se uhvatili u korak i zadržali se u ekosustavu mobilnog plaćanja. Koriste svoju trenutnu stručnost i ulaganje u razvoj sigurnosti i zaštite mobilnih isplata kao obrambena taktika od napadača, [2].

4.2.3. Agregatori

Agregatori su davatelji usluga koji omogućuju obradu između trgovaca i internet trgovine te objedinjuje njihove platne transakcije. U ICT vrijednosnom lancu također se nalaze na strani ponude usluga. Agregatori omogućavaju trgovcima prihvaćanje kreditnih kartica i bankovne transfere bez otvaranja računa trgovca u banci ili udruživanje kartica. PayPal je najpopularniji agregator u svijetu. PayPal američka je tvrtka koja upravlja svjetskim sistemom plaćanja putem Interneta koji podržava Internetski prijenos novca i služi kao elektronička alternativa tradicionalnim papirnatim metodama poput čekova i novčanih naloga.

PayPal djeluje kao posrednik između trgovaca i banaka ili tvrtki koje nude kreditne kartice. PayPal je vrsta „klijent-klijentu P2P (*eng. Peer-to-Peer*)“ usluge. P2P način plaćanja omogućava bilo kome tko ima e-mail adresu da pošalje novac nekom drugom tko također ima e-mail adresu. Inicijalizator transakcije preko PayPala se mora prvo registrirati na PayPal stranicama, te zatim prebaciti određenu svotu novaca na svoj korisnički račun. Korisnik odabire način plaćanja s raznih izvora (slika 21); kreditna kartica, bankovni račun ili direktno PayPal plaćanje. Nakon čega PayPal šalje novac bez da dijeli ostale informacije o svojim korisnicima. Na kraju novac može doći do raznih odredišta ovisno o namjeni kupca da šalje novac drugim ljudima, kupuje nešto na Internetu ili ako kupuje proizvode i usluge na nekim stranicama Internet trgovine, [2].



Slika 21: Slika prikazuje kako funkcionira PayPal aplikacija

Izvor: [14]

PayPal jest pravna organizacija odnosno aplikacija posrednik koja je široko priznata u mnogim zemljama. Stoga je prijenos novca u bilo koju zemlju u njihovoj lokalnoj valuti moguć putem PayPala. Neke su države vrlo stroge jer ne žele da PayPal kao mediji sudjeluje u pranju novca. Stoga se od primatelja uvijek traži izvor sredstava i dokumentacija, [14].

4.2.4. Trgovci

Mobilnim plaćanjem putem prodajnog mjesta POS mogu osigurati bržu propusnost prilikom prolaska kupaca kroz blagajne i mogućnost slanja marketinških poruka u stvarnom vremenu potrošačima. Kao što u ICT vrijednosnom lancu davatelj usluge pruža informacijsko komunikacijske usluge korisnicima putem telekomunikacijskih mreža tako u ekosustavu mobilnog plaćanja trgovac nudi svoje proizvode i usluge, a pomoću mobilnog plaćanja to čini brže i efikasnije. Brži protok se također može postići beskontaktnim karticama i još uvijek nije definirano žele li potrošači zaista cijeniti marketinške poruke u stvarnom vremenu od trgovca na njihovim mobilnim telefonima. Međutim prodajna mjesta mogu imati koristi od mobilnog plaćanja kod smanjenja troškova. Plaćanje putem mobilne telefonije pruža još jedan kanal za trgovce. Telefoni opremljeni NFC-om mogu omogućiti brze i značajne vrijednosti transakcija. Svi oblici plaćanja imaju prednosti i nedostatke: plaćanje gotovinom je sporo i nema koristi ako se misli plaćati na daljinu, a kreditne kartice zahtijevaju PIN ili potpise; ali beskontaktno plaćanje zahtijeva samo karticu ili uređaj s kompatibilnim čitačem. Temeljna prednost kod nekih beskontaktnih platnih sustava za pametne telefone jest da limit potrošnje može biti jednak ograničenju kreditne ili debitne kartice vlasnika računa. Za usporedbu beskontaktne kartice obično imaju prag plaćanja (obično ispod 150 kuna) i ograničenje transakcije prije nego što je potrebna dodatna identifikacija, kako bi se umanjila šteta potencijalno ukradene beskontaktne kartice.

Za prihvaćanje NFC plaćanja trgovcima su potrebni kompatibilni terminali na prodajnom mjestu POS, a novi POS terminali koštaju oko 700 kn što nije preskupa investicija još ako se uzme u obzir da većina trgovaca ima POS uređaj od ranije. Od početka 2015. u svijetu su već postojali milijuni NFC spremnih terminala za plaćanje, od više desetaka milijuna terminala koji se koriste širom svijeta. Za većinu stranaka koje su uključene u prihvaćanje NFC mobilnih plaćanja, razlog za prihvaćanje je financijski. Trgovci da bi potaknuli potrošače na korištenje

mobilnog plaćanja odnosno uređaja opremljenih NFC-om moraju proces plaćanja učiniti jednostavnijim, ugodnijim ili pružiti poseban poticaj u obliku digitalnih kupona ili popusta.

4.2.5. Platne mreže

Funkcioniraju na način da ako korisnik kupi nešto koristeći neki oblik mobilnog plaćanja za 100 kn, trgovac obično prima samo 98 kn. Preostalih 2%, tj. 2 kn naziva se diskontnom stopom, a te 2 kn podijeljene su između svih sudionika koji pružaju uslugu obrade kreditnih kartica. Podjela po sudionicima ekosustava mobilnog plaćanja može biti sljedeća;

- Banka izdavatelj - 1,70 kn (nazvano naknadom za razmjenu, obično 1,7%)
- Mreže za plaćanje, tj. Visa, MasterCard. - 0,10 kn (Fiksna naknada na temelju volumena transakcije tj. 0,10 kn)
- Banka kupca ili trgovačka banka - 0,20 kn (naknada ili postotak na temelju ugovora o trgovačkom kupac-trgovac odnosu tj. obično 0,2%)

U ovom primjeru diskontna stopa iznosi 2%, a u stvarnosti ta diskontna stopa ovisi o vrsti i prirodi transakcije. Općenito sigurnija transakcija jednako niža stopa popusta. Također će transakcija s kreditnim karticama na osnovi čipa imati manju diskontnu stopu, npr. 1,97% nego na kartici koja se ne temelji na čipu. To je zato što se pretpostavlja da što je sigurnija transakcija, to je manji rizik od napada na tu transakciju. Stvarni vlasnik kreditne kartice vrši autoriziranu transakciju s manjim rizikom koji je obrnuto proporcionalan sigurnosti. Diskontnu stopu postavljaju platne mreže**,** tj. Visa, MasterCard, iako platne mreže dobivaju samo mali dio pune stope.

Platne mreže odlučuju kolika će biti diskontna stopa za korištenje, a ne banke izdavatelja ili banke stjecatelja. U gore navedenom primjeru podjele postotka platna mreža diktira i postavlja diskontnu stopu na 2%, iako platna mreža može dobiti samo 0,10 kn po transakciji od te diskontne stope, a ostatak diskontne stope se dijeli između banke izdavatelja (zamjenska naknada) i banke stjecatelja (trgovačka banka). Tako da platne mreže naplaćuju korištenje mrežne infrastrukture, gotovo poput naplatne kućice pored koje prolazi promet na autocesti. Ne izdaju kreditne kartice nego to radi banka izdavatelj. Jednostavno pružaju brendiranje kartice da bi pokazali da je kartica kompatibilna i da će se obraditi s njihovom određenom mrežom za plaćanje kreditnim karticama, [20].

4.2.6. Korisnici

Korisnik je osoba koja koristi računalo ili mrežni servis. Korisnicima računalnih sustava i softverskih proizvoda uglavnom nedostaje tehnička stručnost potrebna da bi u potpunosti razumjeli svoj rad. Napredni korisnici koriste napredne značajke programa, iako nisu nužno sposobni za računalno programiranje i administraciju sustava. Korisnik često ima korisnički račun i sustav ga identificira korisničkim imenom. Ostali pojmovi za korisničko ime uključuju ime za prijavu, ime zaslona, broj računa , nadimak ili nešto slično, [29].

Korisnici su u pravilu individualci odnosno (adresirano) tržište usluga maksimalni broj ljudi kojima je bitan taj proizvod / usluga. Želja davatelja usluge za što većim brojem ljudi u što manjem vremenu ovisno o uređajima, aplikacijama, tehnologijama, interesima. S obzirom na to da su korisnici u središtu za egzistenciju svakog ICT ekosustava i ekosustava mobilnog plaćanja, promijenio se načini razmišljanja i programera i vlasnika aplikacija. Tako je korisnik postao najbitniji dio ekosustava zato korisnike treba rasporediti tako da se definiraju grupe korisnika sličnih karakteristika. Tako da se može kreirati različite usluge koje odgovaraju pojedinoj grupi. Projektant usluga mora biti svjestan što korisnici žele, a to su, [27];

- personalizacija
- interakcija
- dostupnost
- mobilnost

Također žele da komunikacijsko iskustvo bude prilagođeno njihovom stilu života, a usluge dostupne u bilo koje vrijeme na bilo kojem mjestu. Za razliku od prijašnjih sustava u kojima je mreža bila u središtu te su usluge za sve bile iste. Za uspjeh u današnjem sustavima ICT domene jako je bitno segmentirati korisnike. Iako je zadovoljiti korisnika jako bitno i ostvariti maksimalan profit iz toga bitan dio se odnosi i na to što tvrtke žele, a to su, [27]:

- produktivnost
- jednostavnost
- sigurnost
- pouzdanost

Za tvrtke je najbitnije komunikacija koja povećava produktivnost, povećava efikasnost i smanjuje troškove, a to se sve ostvaruje kvalitetnom segmentacijom korisnika.

Kod usluga mobilnog plaćanja jako je bitna segmentacija korisnika prema životnoj dobi. Jer je poznato da se korisnici mlađe životne dobi jako dobro snalaze s novim tehnologijama i lako prihvaćaju neke promjene te čak i teže stalnom ažuriranju sustava i aplikacija za mobilno plaćanja. Dok korisnici starije životne dobi sve to smatraju čudnim i nepotrebnim. Na davateljima usluga i aplikacija te programerima je da prilikom projektiranja neke usluge ili aplikacije nastoje prilagoditi usluge za korisnike svih životnih dobi, te tako povećanjem populacije koja koristi njihove usluge povećavaju opseg korištenja usluge, a kao produkt svega ostvaruju veću financijsku dobit. Segmentacija korisnika na 5 osnovnih dijelova koja vrijedi za svaki ICT ekosustav pa tako i za ekosustav mobilnog plaćanja je sljedeća, [27]:

1. Pioniri (eng. *Pioneers*) predstavljaju prve korisnike usluge koji su zainteresirani za sve nove tehnologije, eksperimentirat će s tehnologijom i biti inspiracija ostalima.
2. Materijalisti (eng. Materialists) sebi orijentirani no manje otvoreni od pionira, međutim rani korisnici usluge, zabava je ono što ih vodi (igre, aplikacije).
3. Društvenjaci (Sociables) pozitivan stav prema tehnologiji i novim uslugama, relativno rani korisnici.
4. Dostizatelji (Achievers) slično materijalistima, sebi orijentirani, preferiraju tradicionalne statusne simbole (automobili, odjeća), koriste tehnologiju i nove usluge većinom kako bi impresionirali okolinu (manje zbog funkcionalnosti).
5. Tradicionalisti zadnji segment u prihvaćanju novih usluga, korištenje novih usluga i tehnologije u onom slučaju kada je to izričito potrebno.

Analizom cjelokupnog ICT ekosustava i ekosustava mobilnog plaćanja dolazimo do zaključka kako su to 2 složena sustava s mnogo sudionika vrijednosnog lanca, gdje na svakog pojedinačno treba detaljno analizirati kako bi u konačnici sveukupan sustav imao smisla. Istraživanjem oba sustava može se zaključiti kako projektanti budućih ICT ekosustava moraju proći kroz analizu svakog pojedinog sudionika, cilj ovoga rada jest da se budućim projektantima pokaže detaljnije o svakoj karici vrijednosnog lanca po nešto, tako kada jednom budu projektirali novi proizvod ili uslugu rad im može poslužiti kao podloga da svoju uslugu razviju bolje i točnije, te da imaju u vidu kroz što sve moraju proći kako bi obuhvatili cijeli ekosustav ICT tržišta.

Počevši od korisnika koje treba kvalitetno segmentirati i raščlaniti korisnika, korisničko ponašanje i korisničku vrijednost, kako bi se postiglo maksimalno zadovoljstvo korisnika. Dalje

bitan dio lanca vrijednosti je koji terminalni uređaj korisnici koriste, je li to mobilni uređaj, pametni sat, tablet ili nešto drugo. Kada ustanove koje terminalne uređaje većina korisnika koristi potrebno je odrediti najčešće korištenu i najisplativiju mrežu pomoću koje će korisnici moći ostvariti komunikaciju za obavljanje mobilnog plaćanja ili nekih drugih funkcija koje usluga nudi. Mreža može biti NFC za beskontaktno plaćanje, ako korisnici često borave kod kuće za zaključiti je da koriste LAN mrežu preko mobilnog uređaja, laptopa ili nekog drugog terminalnog uređaja, a ako su u pokretu treba im omogućiti neki oblik usluge iz domene pokretne GSM mreže.

Kada govorimo o poslužiteljima pristupnik plaćanja ili poslužitelj je odgovoran za sigurno prikupljanje podataka o klijentima na prednjem dijelu aplikacije i potom slanje banci koja ga prima ili platnom procesu kako bi obavio transakciju tako je bitno kojeg poslužitelja odabrati. I na kraju sadržaj koji se prenosi kao jedan od najbitnijih dijelova ekosustava te ono zbog čega aplikacija i postoji jer se upravo zbog sadržaja aplikacije preuzimaju tako da on predstavlja okidač za potencijalnog korisnika usluge da preuzme baš tu uslugu, tako da se sadržaju treba posvetiti dosta pažnje da bude što kvalitetniji i da što bolje opisuje aplikaciju ili uslugu.

5. SIGURNOST I ZAŠTITA USLUGA MOBILNOG PLAĆANJA

Opasnost od upotrebe mobilnog plaćanja leži u tome što potrošači ne brinu mnogo o zaštiti osobnih podataka i sigurnosti telefona. Postoji puno koraka za zaštitu pametnih telefona koji se mogu poduzeti. Prvo korisnici mogu dodati PIN kodove, lozinke i zaključavanje pomoću biometrijske zaštite kao što su otisci prstiju ili tehnologija prepoznavanja lica. Zatim korisnici pametnih telefona mogu instalirati aplikacije za daljinsko praćenje u slučaju da telefon bude izgubljen ili ukraden. Treće, postoje i nadzorne aplikacije za brisanje ili aplikacije koje prate tipično ponašanje telefona i blokiraju aplikacije za plaćanje ako se otkrije sumnjivo ponašanje telefona. Na kraju, korisnici mogu zaključati mobilne novčanike lozinkom ili tehnologijom otiska prsta.

Primjena europskog okvira zaštite podataka započinje pitanjem postoji li obrada osobnih podataka. Definicija osobnih podataka je široka, tj. Bilo koje informacije koje se odnose na identificiranje ili prepoznavanje fizička osoba. Pitanje je li određena vrsta podataka kvalificirani kao osobni podaci mogu zahtijevati detaljnu analizu, uključujući pravnu značajku na koju se može odgovoriti samo na odgovarajući način kada se razmatra specifičan kontekst u kojem se odvija obrada informacija. Kada aplikacija prikuplja podatke s mobilnog uređaja, upotreba

mobilnog uređaja podrazumijeva da se takvi podaci moraju smatrati osobnim podacima u smislu značenja GDPR (eng. *General Data Protection Regulation*). Ne samo podaci na uređaju koji su po svojoj prirodi osobni i privatni, poput slika, poruka, e-poruke, rasporeda korištenja uređaja itd. Nego se i ostali klasificiraju kao osobni podaci, to su npr. podatci na uređaju poput; identifikatora uređaja, aspekte okoline kao što su lokacije uređaja i podataka koji se odnose na njegovu upotrebu, uključujući zapisnike koji sadrže podatke o upotrebi koji se odnose na određene aplikacije. Jednom kada programer aplikacije prikupi (i dalje obrađuje) podatke s uređaja uključujući metapodatke koji se odnose na uređaj i ponašanje korisnika i sve ključne zahtjeve za zaštitu podataka aktivira se GDPR. Kada se govori o GDPR zaštiti podataka treba spomenuti pseudonimne podatke koji predstavljaju novi podskup osobnih podataka koji su u pravnom smislu uneseni u GDPR. Po definiciji GDPR, pseudonimizacija znači obradu osobnih podataka na način koji se osobni podaci više ne mogu pripisati određenom korisniku podataka bez korištenja dodatnih informacija pod uvjetom da se dodatne informacije čuvaju odvojeno i podliježu tehničkim i organizacijskim mjerama koje treba poduzeti i osigurati da se osobni podaci pripišu identificiranoj ili prepoznatljivoj fizičkoj osobi. Pseudonimni podaci i dalje su osobni podaci, a proces pseudonimizacije samo je mjera koju GDPR potiče s obzirom na prednosti za privatnost i sigurnost podataka, [24].

5.1. Prijetnje i napadi na ekosustav mobilnog plaćanja

Najčešći i najlakši oblik napada jest **neovlašteni pristup** izgubljenom ili ukradenom mobilnom uređaju. Izravni napadi pretpostavljaju da napadač posjeduje uređaj koji korisnik nehotice izgubi. Nakon što posjeduju uređaj, napadač će pokušati pristupiti uređaju. Najvjerojatnije napadi sastoje se od pokušaja zaobilaženja bilo kojeg oblika zaštite PIN-a ili zaštite otiskom prsta. Kad je uređaj zaštićen provjerom autentičnosti otiska prsta, napadač se također može poslužiti otiscima prstiju ukradeni iz drugih izvora podataka o otiscima prstiju, npr. podizanje latentnih otisaka s površine. Napadač koji posjeduje uređaj može pokušati upotrijebiti komercijalne ili *open source* forenzičke alate koji zaobilaze PIN-ove, lozinke i ostale oblike zaštite te dobiti korijenski pristup datotečnom sustavu za krađu podataka instaliranih na uređaju. Na aplikacijama je da takve napadače maksimalno ograniče u njihovim namjerama raznim postupcima kao što su udaljeno brisanje osjetljivih informacija ili zaključavanje ukradenog telefona s nekog drugog pouzdanog uređaja na daljinu ili neki drugi oblik zaštite koji će se navesti dalje u radu, [24].

Instalacija zlonamjernog softvera na uređaju sljedeći je oblik napada koji napadači vrlo aktivno koriste. Zlonamjerni softver" je svaki softver koji je dizajniran da našteti uređaju. Zlonamjerni softver može ukrasti osjetljive podatke s mobilnog uređaja i postupno usporiti računalo, pa čak i slati lažne poruke e-pošte s korisnikovog računa e-pošte, često bez znanja legitimnog korisnika o tome što se događa. Ovo je nekoliko uobičajenih vrsta zlonamjernog softvera, [24]:

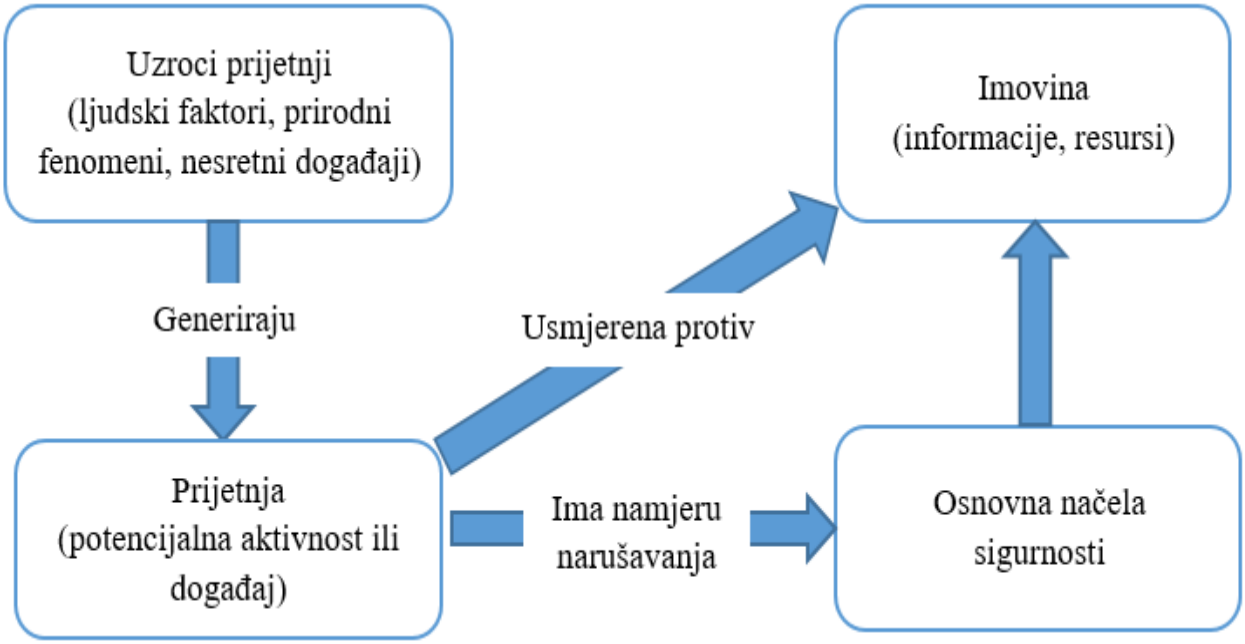
- virus: štetni računalni program koji se može kopirati na računalo i zaraziti ga.
- crv: zlonamjerni računalni program koji putem mreže šalje kopije sebe na druga računala.
- spyware: zlonamjerni softver koji prikuplja podatke o korisnicima bez njihova znanja.
- adware: softver koji automatski preuzima oglase na računalo, pokreće ih ili prikazuje.
- trojanac: destruktivni program koji se maskira kao korisna aplikacija, međutim nakon instalacije šteti računalu ili krade informacije.

Obrnuti inženjering izvornog koda aplikacije je jedan od složenijih napada riječ je o načinu kada napadač stvara scenarij u kojem je on izvor informacija koje žrtvi trebaju, te ona pristupa napadaču. Napadač stvori scenarij gdje je on osoba koju će zaposlenici pitati za određene informacije. Ako je dobro istražio i pripremio se, napadač reverznim socijalnim inženjeringom ima povećane šanse za dobiti potrebne informacije od zaposlenika. Tri su dijela obrnutog socijalnog inženjeringa: sabotaža, oglašavanje i pomaganje. Najbolji primjer je sljedeće: napadač sabotira mrežu određene organizacije, što prouzrokuje problem. Zatim se oglasi kao odgovarajuća osoba za rješenje tog problema, a zatim kada dođe popraviti problem zahtjeva određene informacije od zaposlenika i tako dobije ono što je otpočetka i želio, a zaposlenici i organizacija nikada ni ne saznaju da je bila riječ o napadu, jer im je mreža stvarno popravljena, [24].

Neovlašteno preuzimanje informacija putem aplikacije za plaćanje mobilnim uređajem. Napadač može odlučiti preusmjeriti mobilni zahtjev za plaćanje kako bi zabilježio podatke za prijavu i preusmjerio ih na poslužitelj koji on kontrolira. To bi učinio preuzimanjem legitimne prijave s trgovina za mobilno plaćanje raspakiravanje relevantnih rutina i zatim prepakiravanjem radi daljnjeg napada. S obzirom na to da danas postoji milijun aplikacija koje podržavaju mobilno plaćanje ili nude uslugu mobilnog plaćanja ovo je jedan od čestih napada, [24].

Phishing i socijalni inženjering jesu napadi na aplikacije. Mobilni telefoni kombiniraju osobnu i korporativnu upotrebu. Mobilni uređaji skupljaju sve više i više informacija o kupcima odnosno korisnicima, a skupljene bi informacije mogle pomoći u obavljanju sofisticiranih napada. Ovi napadi ciljaju na krađu korisnikova identiteta i socijalnim inženjeringom iskorištavajući različite komunikacijske kanale (npr. telefon, e-pošta, SMS) te podatke o korisniku dostupne u javnoj domeni (npr. društveni mediji web stranice, tražilice). Podaci koje traže napadači koji se koriste socijalnim inženjeringom često su podaci o kreditnim karticama i osobni podaci o kojima korisnik raspolaže. Ukradeni podaci o kreditnoj / debitnoj kartici ili unaprijed plaćenim karticama može se unovčiti ili upotrijebiti za prevaru plaćanja. Ukradeni osobni podaci korisnika mobilnog plaćanja (npr. imena, prezime, datum rođenja, kontakt informacije kao što su adresa za dostavu računa, e-poruke, telefonski brojevi) mogu se koristiti za lažno predstavljanje napada i za krađu identiteta. Postoje razni načini ovakvih napada za koje korisnici uopće nisu svjesni, niti upoznati na koje sve načine i koliko izlažu svoje podatke kroz razne aplikacije i online sadržaje, [24].

Instalacija aplikacija za praćenje i zlonamjernog softvera je još jedan od mogućih napada na aplikacije. Nesigurne WiFi točke (npr. Internet kafića, javnih mjesta, shopping centara i dr.) koji napadaču mogu omogućiti ciljanje mobilnog uređaja s *Man-in-The-Middle* napadom. Također postoji mogućnost napada mreže podmetanjem. To je slučaj kada zlonamjerni korisnik postavi lažnu pristupnu točku s istim mrežnim nazivom, kao onu koja već postoji, poput popularnog naziva kafića ili tržišnog lanca. Mogli bi postaviti lažnu web stranicu kako bi se "autentificirali" korisnici i tako prikupljali podatke, a oni će ih kasnije moći koristiti za sljedeće korake napada. Nije neuobičajeno da mnogi ljudi koriste isto korisničko ime i lozinku za više različitih usluga, čak i za mobilni zahtjev za plaćanje. Prethodno navedeno napadačima olakšava proces napada, zato se preporučuje mijenjanje lozinki za svaku pojedinu aplikaciju te da se ne koriste inicijali imena, prezimena ili datuma rođenja za PIN-ove i lozinke, [24].



Slika 22: Odnosi između uzroka prijetnje, prijetnje i osnovnih načela

Izvor [30]

Prijetnja (eng. Threat) predstavlja okolnost ili pojavu koja ima potencijal uzrokovati štetu ili gubitak. Prijetnja se sastoji od potencijalne aktivnosti ili pojave koja može negativno utjecati na osnovna načela informacijske sigurnosti. Prijetnje se na javljaju samostalno već moraju sadržavati uzroke. Uzorci prijetnje mogu biti predstavljeni ljudskim (slika 22) faktorom ili prirodnom pojavom ili nesretnim događajem.

5.2. Metode zaštite i ranjivosti ekosustava mobilnog plaćanja

Svaka strana uključena u ekosustav mobilnog plaćanja trebala bi pokazati dokaze o isporučivanju informacija na siguran način. To uključuje ne samo pružatelja usluga mobilnog plaćanja, već i ključne čimbenike kao što su TSP (davatelji usluga tokena čija su arhitektura i princip rada objašnjeni u 3. poglavlju rada) i baze podataka u oblaku. Važno je da se sigurnosni pregled s kraja do kraja ne provodi izolirano, gdje se svaki element preispituje, nego se mora ostvariti povezanost između sudionika kako bi se lakše zaštitili od napada. Stoga je potrebno da različiti sudionici ekosustava mobilnog plaćanja surađuju ne samo u integraciji i pružanju usluge,

već i u osiguravanju zajedničkog cilja prema povećanju sigurnosti. Također je ključno pregledati sve najčešće prijetnje. Davatelji mobilnih plaćanja trebali bi upozoriti kupce i trgovce na rizike i posljedice pokretanje njihove aplikacije u mobilnom okruženju.

Kupci bi trebali slijediti niz minimalnih sigurnosnih mjera koje trebaju biti potrebne za sigurno korištenje njihove aplikacije, [25];

- kupac bi trebao ažurirati operativni sustav na redovnoj osnovi čim OS pruža dostupno ažuriranje,
- ograničiti obavljanje mobilnih platnih transakcija s računa nepouzdana mreža (poput javne WIFI pristupne točke) te tako onemogućiti presretanje trećih strana,
- autentifikacija kupca na mobilnom uređaju uvijek se mora provoditi uporabom biometrijske kontrole ili jakog PIN-a, uzorka ili zaporke i
- učinkovita konfiguracija treba biti uspostavljena u slučaju gubitka ili ugrožavanja uređaja, jedna od mjere je uklanjanje podataka na daljinu.

Trgovci također da bi zaštitili svoje transakcije i cjelokupno mobilno poslovanje trebaju slijediti upute koje se odnose na zaštitu njihovog ekosustava, [25];

- POS softver trebao bi se ažurirati čim pružatelj ponudi sigurnosno ažuriranje. POS softver ima vidljivost svih platnih transakcija i stoga je glavna meta napada.
- POS se može mijenjati s hardverske perspektive, tako da treba podići svjesnost trgovca o mogućnostima napada te da se mijenjanjem hardvera također može podići razina sigurnosti.

Dodatne mjere koje trgovci trebaju primijeniti su korištenje tehnika vraćanje i backupa podataka. Kad je moguće provjeravanje integriteta pokrenutog koda, kako bi se osiguralo da nije bilo nikakvih napada. Kad je moguće u svakom trenutku minimiziranje potencijalnih MTM napada. I svakako implementirati učinkovito korištenje certifikata kako bi se osiguralo da aplikacija komunicira do predviđenih krajnjih točaka te da se ne izlaže riziku, [25].

Mobilni uređaj kao jedan od glavnih sudionika u ekosustavu mobilnog poslovanja treba zaštiti od raznih prijetnji, kao što su krađa identiteta, socijalni inženjering, instalacija zlonamjernih aplikacija itd. Sve navedene prijetnje mogu se dogoditi zbog; nepažnje prilikom pregleda e-mail poruka, otvaranjem sumnjivih SMS poruka, *download* sumnjivih aplikacija, korištenje javno dostupnih Wi-Fi mreža i nepridržavanje minimalnih mjera potrebnih za sigurnost. Zaštita i mjere koje se mogu poduzeti su; svjesnost korisnika mobilnog uređaja o

prijetnjama, redovno ažuriranje operativnog sustava i povremeni backup podataka na neke druge uređaje ili sigurne *Cloud* servere, [25].

Mobilno plaćanje i digitalni novčanik su dio ekosustava koji je također izložen prijetnjama kao što su obrnuti inženjering kako bi se došlo do izvornog koda aplikacije i krađa transakcija mobilnih plaćanja. Ranjivost ovih sustava jesu onemogućavanje izvornog koda aplikacije, krađa privatnih ključeva, dodavanje ukradene kreditne kartice, lažno predstavljanje te korištenje slabosti kod biometrijskih i drugih oblika autorizacije. Mjere zaštite koje bi se trebale provoditi radi zaštite digitalnog novčanika i mobilnog plaćanja su; obučavanje zaposlenih i praksa o digitalnom kodiranju (priručnici i razni alati), zaštita od pogrešaka sustava, razne kriptografske metode te korištenjem sigurnih aplikacija digitalnog novčanika i mobilnog plaćanja općenito, prijava neovlaštenih aplikacija, korištenje raznih potvrda i zaštita identiteta, [25].

Banka (stjecatelj i izdavatelj) prijetnje predstavlja obrada podataka za plaćanje i čuvanje istih na sigurnom mjestu gdje postoji mogućnost da se instalira maliciozni kod ili softver u bazu podataka ili *Cloud* server gdje se sve transakcije obrađuju. Prijetnju predstavlja i neovlašteni pristup te iskorištavanje slabosti u izvršenju unutarnjih sigurnosnih kontrola i mjera za pristup sustavu. Dalje ranjivost predstavljaju curenje podataka, otkrivanje podataka zbog slabe zaštite servera za obradu. Ranjivosti kod ovog sustava su još praznine u potvrđivanju autorizacije kao što su provjera i potvrda, sumnjive transakcije i digitalni potpis. Mjere sigurnosti i zaštite koje sve banke provode su jačanje sigurnosti sustava za obradu podataka, dvostruka provjera autentičnosti korisnika. Posjedovanje programa i alata za otkrivanje zlonamjernog softvera i mjesta curenja podataka, posjedovanje sigurne pristupne točke i Interneta te zahtijevanje digitalnog potpisa od svih kupaca, [25].

Platna mreža da bi platna mreža posjedovala visoki stupanj zaštite mora dobro i sigurno komunicirati sa tokenskim TSP sustavom i provoditi sve korake koji su nabrojani kod tokenskog sustava. Tako da ranjivost ovog sustava predstavlja pogrešna konfiguracija tokenskog poslužitelja, nevaljani spremnik sigurnosnih i kriptografskih ključeva. Ranjivost predstavlja svakako i razmjena osjetljivih PAN brojeva te nesigurna veza između stjecateljske i izdavateljske banke kojima platna mreža djeluje kao posrednik. Jedan od čestih napada na platne mreže jest DOS (eng. Denial of Service) gdje se nastoji onemogućiti tokenski server. Mjere zaštite koje se provode su sigurnosna konfiguracija i jačanje sigurnosnih servera platnih mreža, sigurna pohrana kriptografskih ključeva, dvostruka autentifikacija i kontrola za pristup tokenskom sustavu, [25].

Bez obzira na tehnologiju i način mobilnog plaćanja postoje minimalni zahtjevi zaštite i sigurnosti zbog osjetljivosti transakcija mobilnog plaćanja koje bi svaki sustav i aplikacija morali zadovoljiti, [26];

- **identifikacija** kao rješenje za mobilno plaćanje treba moći identificirati entitete i subjekte koji su uključeni u proces plaćanja. Da bi se ostvario ovaj zahtjev svaki bi subjekt trebao imati jedinstveni identifikator. U sustav mobilnog plaćanja postoje broj mobilnog telefona, korisnikov ID ili broj bankovnog računa koji se klasificiraju kao identifikatori.
- **autentifikacija** kao dokaz identiteta jednako je važan kao i identifikacija; stoga sustav treba imati odgovarajuća sredstva za osiguranje da korisnik stvarno predstavlja osobu za koju tvrdi da jest. Tri faktora omogućuju sustavu provjeru identitet subjekta: nešto što ima (npr. token, pametna kartica, potvrda), nešto što zna (npr. zaporka, osobni identifikacijski broj (PIN)) ili nešto što jest (npr. otisak prsta, glas, uzorak mrežnice i sl.)
- **autorizacija** ograničenja i uspostava minimalnih razina privilegija svakoj strani zbog uspješnog izvršavanje transakcija i kontrole nad pristupom informacijama koje se prijenose u procesu mobilnog plaćanja.
- **integritet** da bi se očuvala cjelovitost podataka između dvije strane koje sudjeluju u procesu mobilnog plaćanja, to uključuje izbjegavanje izmjena podataka dok prolaze mrežom ili dok su pohranjeni.
- **povjerljivost** znači da podatci ne budu mijenjani niti modificirani te da ostanu privatni kako bi se izbjegla njihova zloupotreba. To se postiže enkripcijom.
- **mehanizmi revizije i nepotvrđivanje** za potrebe revizije evidencija izvršenih transakcija je obavezna. Podaci o evidencija mogu sadržavati jedinstveni identifikator, vremenske oznake, trgovce uključene u proces mobilnog plaćanja i vrijednosti transakcije.

S obzirom na to da obje kriptografske metode (asimetrična i simetrična kriptografija) imaju svojih prednosti i nedostataka, najbolje rješenje za sigurnost ekosustava mobilnog plaćanja predstavlja kombinacija ovih dviju metoda kako bi se sigurnost stavila na najviši nivo što je PKI (eng. *Public Key Infrastructure*) i učinio. PKI je skup hardvera, softvera, ljudi, politika i postupaka potrebnih za stvaranje, upravljanje, distribuciju, upotrebu, pohranu i opoziv digitalnih

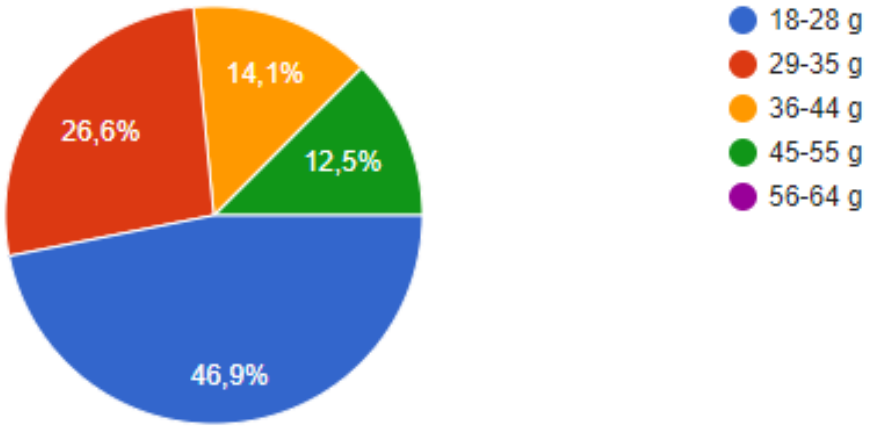
potvrda. PKI je također ono što veže ključeve s identitetom korisnika putem certifikata. PKI koristi hibridni kripto sistem i koristi se od obje vrste enkripcije. Primjer navedenog PKI može se vidjeti kod SSL (eng. *Secure Sockets Layer*) standardna sigurnosna tehnologija za uspostavljanje šifrirane veze između poslužitelja i klijenta obično web poslužitelj (web stranica) i preglednik ili poslužitelja e-pošte i klijent e-pošte. I to se smatra najboljim i najprihvaćenijim oblikom zaštite uz tokenski sustav koji se koristi u svim načinima i aplikacijama mobilnog plaćanja.

6. REZULTATI ISTRAŽIVANJA PROVEDBOM ANKETE

Istraživanje je provedeno da bi se uvidjele potrebe korisnika za uslugama mobilnog plaćanja, te njihovo zadovoljstvo takvim načinom plaćanja te se na temelju istraženog želi uvidjeti što korisnici smatraju korisnim, a što bi još trebalo unaprijediti. U anketi su bili uključeni razna pitanja kao što su dob korisnika, razina obrazovanja korisnika, koliko često idu u banku, koji uređaj koriste, znaju li uopće da njihov uređaj posjeduje NFC tehnologiju i jedno od najvažnijih pitanja smatraju li mobilno plaćanje sigurnim i jesu li u budućnosti spremni fizički plaćati mobilnim uređajem.

Metoda anketiranja provedena je online u *Facebook* grupama ciljano gdje se nalaze mlađi korisnici odnosno studenti, jer s obzirom na korištenje mobitela i snalažljivost s uslugama mobilnog plaćanja najobjektivnije odgovore i najtočnije provođenje ankete o analizi usluga mobilnog plaćanja se može očekivati od mlađe populacije. No s obzirom na to da Internet i njegovu nepredvidivost nisu samo glasale osobe u rasponu godina (18-28) već i nešto starija populacija, tako da je istraživanje provedeno u potpunosti i s jasnijim rezultatima. U anketi je sudjelovalo 64 ispitanika, od čega je bilo 38, odnosno 59,4 % žena i 26, odnosno 40,6 % muškaraca

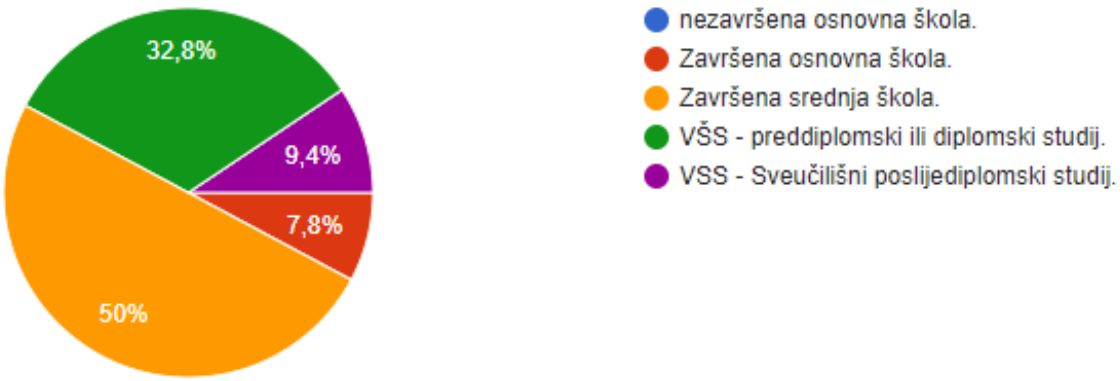
Sljedeće pitanje se odnosilo na raspon godina ispitanika koji je bio poredan na sljedeći način: 18-28, 29-35, 36-44, 45-55, 56-64. Najveći broj ispitanika bio je u starosnoj skupini 18-28, u postotcima 46,9%, zatim ga je pratila skupna 29-35 sa 26,6%. U skupini 36-44 bilo je 14,1% ispitanika, dok u skupini 45-55 bilo čak 8 ispitanika, odnosno 12,5% osoba, u skupini 56-64 nije bilo ispitanika prikazano u grafikonu 2.



Grafikon 1: Raspon godina ispitanika

Iz grafikona 1 je vidljivo da je najveći broj ispitanika koji su ispunili anketu u rasponu godina od 18-28 i 29-35. Iz navedenog se može zaključiti da je anketa uspješno provedena jer je ciljana skupina bila mlađa populacija, s obzirom na to da je pretpostavka da oni mnogo više koriste mobilni uređaj i sve njegove prednosti i funkcionalnosti, pa ga tako koriste i za mobilno plaćanje više nego starije osobe.

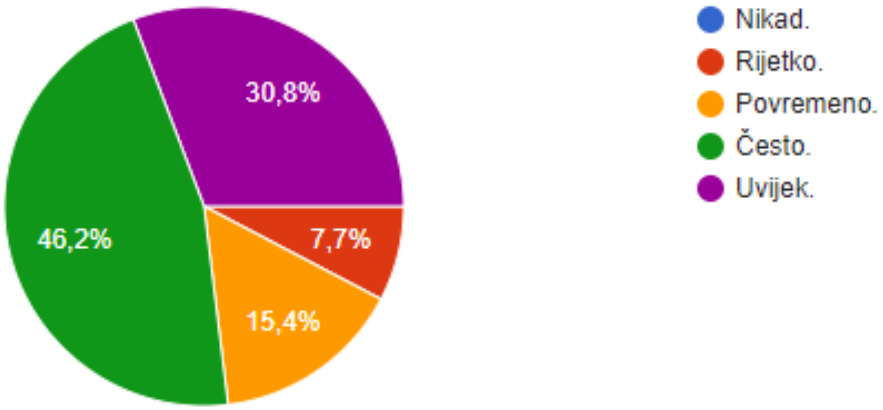
Sljedeće pitanje se odnosilo na najviši stupanj obrazovanja kojeg su ispitanici postigli čiji se rezultat vidi na grafikonu 2.



Grafikon 2: Završeni stupanj obrazovanja ispitanika

Najveći broj ispitanika čak njih 50% ima završeno srednju školu, ali s obzirom na to da je istraživanje provedeno u srpnju većina ispitanika je taman završila srednju školu i planira upisati fakultet, nezavršenu osnovnu školu nema niti jedan ispitanik što je i očekivano, dok završenu samo osnovnu škol ima 7,8 % ispitanika što su vjerojatno starije osobe. Višu stručnu spremu (VŠS) ima 32,8 % ispitanika, a VSS ima 9,4 % ispitanika što u sumi daje 27 visoko obrazovanih ispitanika koji se sigurno znaju koristiti mobilnim uređajem i uslugama mobilnog plaćanja.

S obzirom na to da za korištenje usluga mobilnog plaćanja potreban mobilni uređaj sljedeće pitanje bilo je koliko često u danu ispitanici koriste mobilni uređaj.

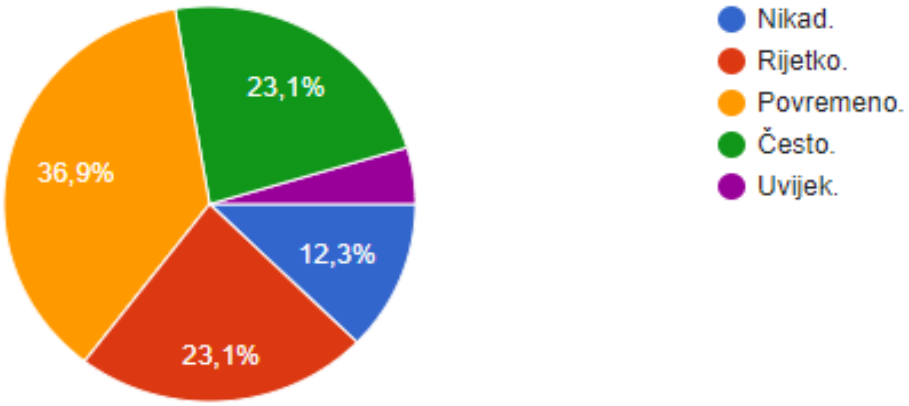


Grafikon 3: Prikaz koliko često korisnici koriste uređaj u danu

Iz grafikona 3 vidljivo je da 77 % ispitanika koriste stalno ili često uređaj u danu što je i normalno zbog ciljano ispitane mlađe populacije kojima je mobilni uređaj gotovo cijeli dan neprekidno u ruci u svim životnim situacijama, pa su na temelju toga i češće u prilici koristiti neki od raznih načina mobilnih plaćanja. Ostalih 15,4 % koriste povremeno mobilni uređaj, dok

njih samo 7,7 % koriste rijetko mobilni uređaj u jednome danu. Dok niti jedna osoba od 64 ispitanika nije navela da uopće ne koristi mobilni uređaj u danu.

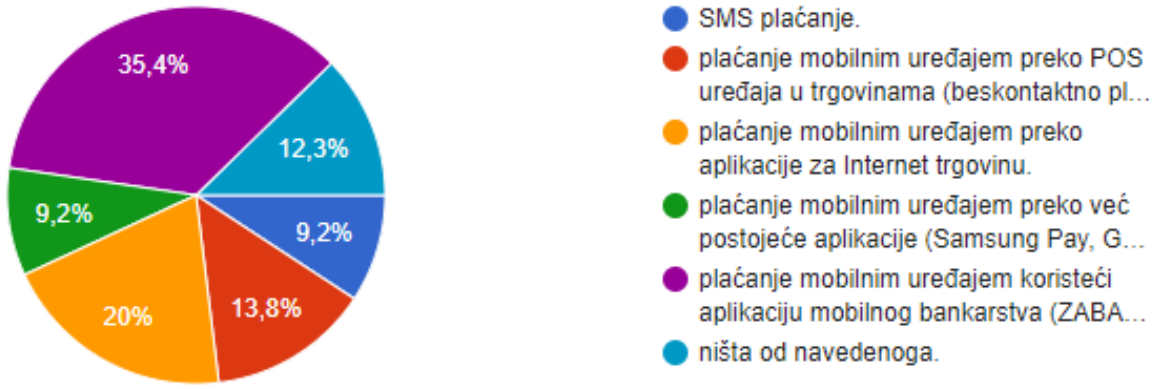
Povezano na prethodno pitanje sljedeće pitanje je glasilo koliko od 64 ispitanika koristi mobilni uređaj za plaćanje nekog proizvoda ili online usluge što je prikazano grafikonom 4.



Grafikon 4: Koliko često ispitanici koriste mobilni uređaj za plaćanje

Zanimljivost kod ovoga pitanja je ta da je čak 12,3 % ispitanika navelo da nikad ne koriste mobilni uređaj za plaćanje nekog proizvoda ili online usluge, a 23,1 % rijetko koriste mobilni uređaj kao način plaćanja, iz čega se može zaključiti kako je mobilno plaćanje još u razvoju i da treba potaknuti i druge dobne skupine na ovaj oblik plaćanja. Povremeno usluge mobilnog plaćanje koristi čak 36,9 % ispitanika što je i za očekivati, jer ispitanici povremeno kad nemaju nikakav drugi način plaćanja posegnu za mobitelom da bi platili npr. bon, parking ili neki proizvod iz online trgovine kojeg nema u njihovoj zemlji. Čak 23,1 % ispitanika koristi često usluge mobilnog plaćanja odnosno 15 ispitanika, dok je 3 ispitanika navelo da uvijek koriste mobilni uređaj za plaćanje nekog proizvoda ili online usluge.

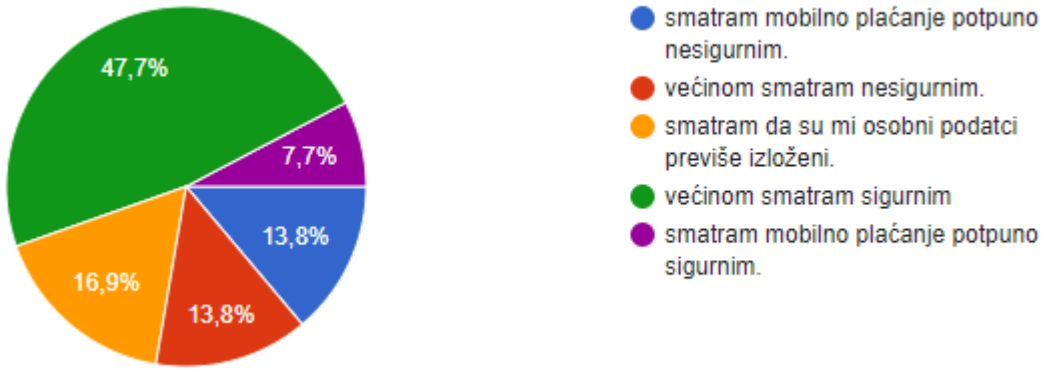
Cilj sljedećeg pitanja bio je ustanoviti koji oblik plaćanja od navedenih u pitanju korisnici najviše koriste i je li uopće koriste nešto od navedenoga što je prikazano na grafikonu 5.



Grafikon 5: Koji oblik plaćanja korisnici najviše koriste

Kod ovoga pitanja pobjedu je uvjerljivo odnijelo plaćanje mobilnim uređajem koristeći aplikaciju mobilnog bankarstva (ZABA, PBZ mobilna aplikacija ili neke druge) odnosno plaćanje pomoću aplikacije koju je ispitanicima omogućila njihova banka čak njih 35,4 % je navelo takav oblik plaćanja. Kad se gleda s aspekta sigurnosti mobilnog plaćanja i obrazovanja ispitanika kod kojih većinom prevladava srednja škola, dolazi se do zaključka da je ovakav odgovor na ovo pitanje i objektivan s obzirom na to da su svi povjerljivi podatci, informacije, bankovni račun i financijska sredstva koji se koriste povezani s bankom ispitanika kojoj oni vjeruju te i ako dođe do nekog sigurnosnog propusta banka ima već opravdane mehanizme i načine da riješi bilo kakav problem ili *cyber* napad i stoga je u prednosti s obzirom na odabir načina plaćanja u odnosu na ostale načine plaćanja koji su također sigurni, ali korisnici nisu dovoljno upoznati sa sigurnosti drugih načina plaćanja te je to jedan od aspekata mobilnog plaćanja kojeg treba bolje predstaviti korisnicima. Iako je očekivano bilo da je sljedeći najzastupljeniji oblik plaćanja SMS plaćanje s obzirom na sigurnost za koju je zadužen mobilni operator i brzinu korištenja ovog načina plaćanja, zanimljivo je da je samo 9,2 % ispitanika navelo SMS plaćanje, a čak 20 % ispitanika je navelo da koristi mobilni uređaj za plaćanje preko aplikacija za Internet trgovinu. Također neočekivan rezultat jest da je čak 9 ispitanika odnosno njih 13,8 % navelo da koriste mobilni uređaj za beskontaktno plaćanje na POS uređaju u trgovinama jer je takav oblik plaćanja iako je moguć još u razvoju kad gledamo hrvatsko tržište. Korištenje mobilnog plaćanja preko već postojeće aplikacije na uređaju npr. Samsung Pay, Google Pay ili Andoroid Pay koristi samo 9,2 % odnosno 6 ispitanika, dok je za ništa od navedenih oblika plaćanja navelo 8 ispitanika odnosno 12,3 %.

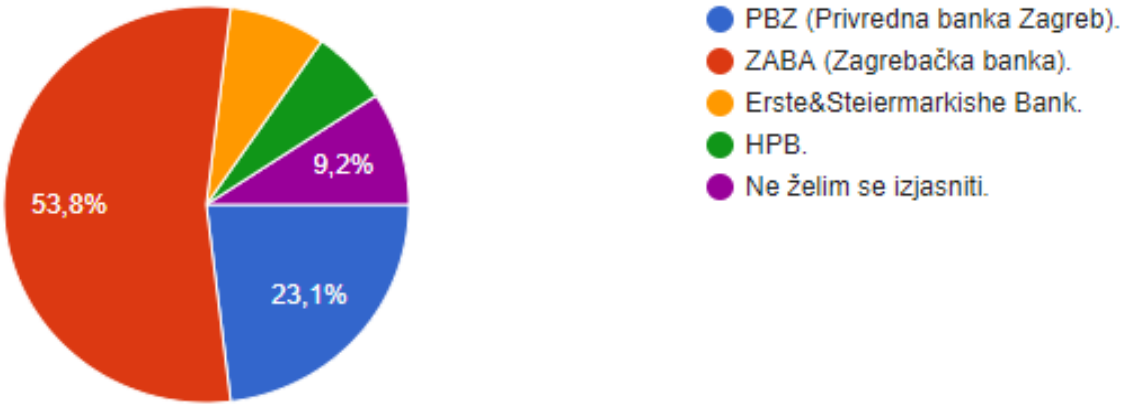
Nakon što se ustanovilo koje oblik plaćanja ispitanici najviše koriste ispitanicima je postavljeno pitanje smatraju li mobilno plaćanje sigurnim što je prikazano na grafikonu 6.



Grafikon 6: Prikazuje koliko ispitanici smatraju mobilno plaćanje sigurnim

Svrha ovoga pitanja je bila ustanoviti koliko ispitanici smatraju mobilno plaćanje sigurnim. Čak 47,7 % ispitanika smatra mobilno plaćanje većinom sigurnim, a 7,7 % ga smatra potpuno sigurnim, iako smo ranije vidjeli da ispitanici većinom vjeruju svojim bankama kad nešto plaćaju iz ovoga pitanja vidimo da više od pola njih smatra da su im podatci potpuno ili većinom sigurni. Potpuno nesigurnim mobilno plaćanje smatra 13,8 % ispitanika, jednaki postotak ispitanika smatra mobilno plaćanje potpuno nesigurnim, a 16,9 % njih smatra da su im podatci previše izloženi, gdje se opet mora spomenuti kao i kod prethodnik pitanja, potreba za povećanjem svjesnosti korisnika o sigurnosti svih načina mobilnog plaćanja i cijelog njegovog ekosustava.

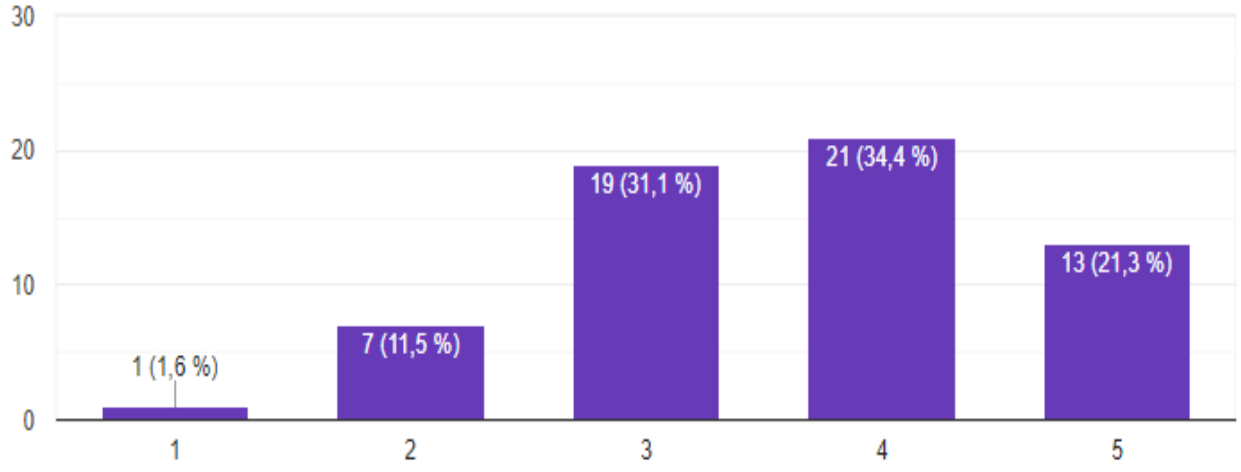
Svrha sljedećeg pitanja je bila saznati koja aplikacija mobilnog bankarstva se najviše koristi kod ispitane skupine, a odgovor na to pitanje se dobio indirektno tako da se postavilo pitanje koju banku od navedenih ispitanici koriste što je prikazano grafikonom 7.



Grafikon 7: Prikazuje koju banku ispitanici koriste

Kao što je i očekivano najveći broj ispitanika čak njih 53,8 % koristi Zagrebačku banku odnosno (ZABA aplikacijsko rješenje Zagrebačke banke), sljedeća banka koju ispitanici najviše koriste je PBZ njih 23,1 % (koja također ima svoje aplikacijsko rješenje za mobilno bankarstvo), ako uzmemo u obzir odgovore iz prethodnih pitanja gdje ispitanici najviše koriste upravo aplikacije za mobilno bankarstvo svojih banaka kao način mobilnog plaćanja, dolazimo do zaključka da ispitanici najviše vjeruju te se osjećaju najsigurnije koristeći takve aplikacije, razlog tomu je kao što je prethodno i navedeno što banke imaju visok stupanj sigurnosti i lojalnosti prema svojim korisnicima, te bi se ostale konkurentne aplikacije ili načini plaćanja trebali usmjeriti prema reklamiranju vlastite sigurnosti i tome koliko brinu o zaštiti osobnih podataka svojih korisnika. Za primjer navedenoga se može uzeti i ovaj rad koji mnogo toga govori o sigurnosti aplikacija Samsung Pay, Android Pay i Google Pay te o sigurnosti mobilnih plaćanja i njegovom ekosustavu općenito.

Nakon što se saznalo koje banke ispitanici koriste te samim time koje aplikacije mobilnog bankarstva koriste, sljedeće zadatak u anketi bio je da ocjene svoju aplikaciju mobilnog bankarstva s obzirom na to da je ovo pitanje bilo opcionalno za unos, jer ne koriste svi aplikaciju mobilnog bankarstva, sudjelovao je 61 ispitanik što znači da od 64 ispitanika samo njih 3 ne koriste usluge mobilnog bankarstva koje im pruža njihova banka i tako je i ovo pitanje pokazatelj kako je anketa uspješno provedena i da je ciljana skupina pogođena što je prikazano grafikonom 8.



Grafikon 8: Prikaz kako ispitanici ocjenjuju aplikaciju mobilnog bankarstva svoje banke

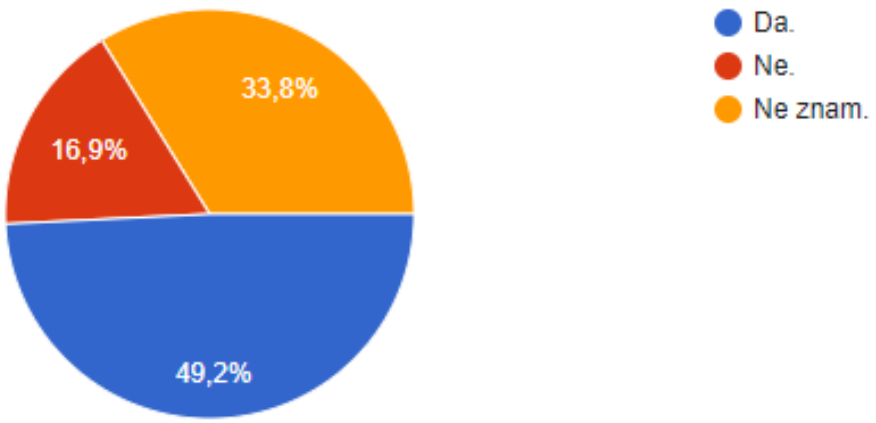
Iz grafikona je vidljivo da su najveće ocjene 3 i 4 dok je 21,3 % dalo ocjenu 5 za svoju aplikaciju mobilnog bankarstva, a 7 ispitanika je dalo ocjenu 2 dok je samo 1 ispitanik negativno ocijenio svoju uslugu mobilnog bankarstva. Iz svega dobivenog da se zaključiti da aplikacije mobilnog bankarstva rade dobar posao, tu se prvenstveno misli na ZABA-u i PBZ mobilno bankarstvo jer se iz prethodnih pitanja vidi da one zajedno čine većinu što se tiče aplikacijskih rješenja, a s obzirom na to da je samo 13 od 61 ispitanika koji su odgovorili na ovo pitanje dalo ocjenu odličan vidi se da kao i kod svih ostalih način plaćanja i ovdje ima mjesta za napredak i poboljšanje.

Kako bi se donio kvalitetan zaključak što je još potrebno aplikacijama da bi ostvarile veće zadovoljstvo korisnika, ispitanicima je postavljeno pitanje što najviše vole kod usluga mobilnog plaćanja rezultat ovoga pitanja prikazan je grafikonom 9.

Grafikon 9: Prikazuje što najviše korisnici vole kod usluga mobilnog plaćanja

Analizom dobivenih rezultata kod ovoga pitanja vidi se da ispitanici najviše vole brzinu plaćanja svojih proizvoda, usluga i ostalih transakcija čak njih 43,8%, bez da moraju čekati u redovima, tako da bi taj dio također bilo dobro reklamirati i staviti naglasak kako se s mobilnim plaćanjem može sve platiti i obaviti sigurno i brzo bez napornog čekanja u redovima i da se svi procesi koji se odvijaju u banci mogu riješiti preko aplikacije za mobilno bankarstvo. Ovakav način plaćanja inovativnim i zanimljivim smatra 21,9 % ispitanika što je u uskoj povezanosti s brzinom plaćanja i obavljanja svih procesa vezanih za plaćanje, jer da nije tako ne bi korisnici mobilno bankarstvo ni smatrali zanimljivim. S kvalitetom usluge je zadovoljno 10,9 % ispitanika dok 9,4 % ispitanih vole to što se ne moraju mučiti s gotovinom. Neočekivan rezultat je da se čak 14,1 % ispitanika izjasnilo da ne koristi ovakav oblik usluga.

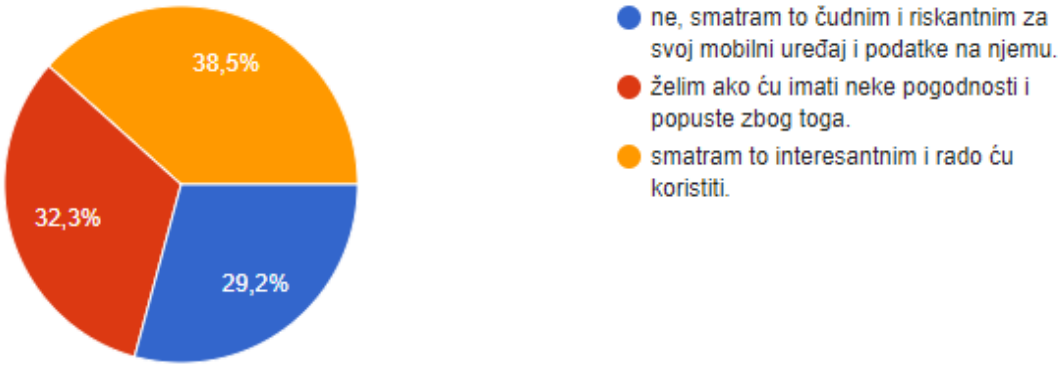
Iz prethodnog pitanja smo ustanovilo se da korisnici najviše vole brzinu obavljanja svih usluga koje im pruža široka „lepeza“ usluga mobilnog plaćanja. Također najviše ispitanih smatra takav oblik plaćanja inovativnim i zanimljivim, pa je sljedeće pitanje usmjereno na tehnologiju kako bi se obuhvatio čitav ekosustav mobilnog plaćanja i da se ustanovi što bi još korisnicima moglo povećati njihovu brzinu obavljanja mobilnih transakcija i učiniti usluge još zanimljivijima. Prethodno navedeno se sigurno može obaviti NFC tehnologijom kao oblikom beskontaktnog plaćanja pa je sljedeće pitanje za ispitanike glasilo je li njihov uređaj posjeduje NFC tehnologiju rezultati pitanja prikazani su na grafikonu 10.



Grafikon 10: Prikaz koliko ispitanika posjeduje NFC tehnologiju

S obzirom na to da danas više ne postoji novi smartphone uređaj koji ne posjeduje NFC tehnologiju rezultati odgovora na ovo pitanje su opravdani, jedino što se može dogoditi je da korisnici nisu dovoljno upoznati sa svojim uređajem te ne znaju da posjeduju NFC tehnologiju i koliko će im ona može biti korisna. Tako da se skoro pola od ispitanika izjasnilo da posjeduje uređaj s NFC tehnologijom njih 49,2 %, ispitanika koji su rekli da ne znaju da im uređaj posjeduje NFC tehnologiju je 33,8 % što je i bila svrha ovog pitanja da se ustanovi koliko od ispitanih ne zna još sve funkcionalnosti svog mobilnog uređaja te je i to jedan dio ekosustava mobilnog plaćanja gdje se može staviti naglasak da se korisnike bolje upozna s funkcijama i tehnologijama koje njihov uređaj posjeduje, a 16,9 % ispitanih je reklo da ne znaju je li im uređaj posjeduje NFC tehnologiju.

Kao završno pitanje na anketi bilo je koliko je korisnika u budućnosti spremno zamijeniti karticu i prisloniti mobilni uređaj na POS uređaj za plaćanje u trgovinama i je li to smatraju sigurnim, što je prikazano grafikonom 11.



Grafikon 11: Prikaz jesu li korisnici spremni koristiti mobilni uređaj za beskontaktno plaćanje

Kao rezultat i zaključak cijelog istraživanja provedbom ankete korisnici su dali odgovor na posljednje pitanje koje je prikazivalo jesu li spremni zamijeniti kreditnu karticu s mobilnim terminalnim uređajem kao oblikom plaćanja na POS uređaju u trgovinama. S obzirom na to da je sve što je novo i čini nek promjenu od normalnog načina funkcioniranja ljudi vrlo brzo prihvate i pokušaju koristiti, pa tek onda nakon nekog vremena odluče je li im se to isplati ili ne, tako je i ovdje kod pitanja jesu li spremni zamijeniti kreditnu karticu i prisloniti mobilni uređaj na POS uređaj za plaćanje njih čak 38,5 % ispitanih odgovorilo da smatraju to interesantnim i da će to rado koristiti. Veliki broj ispitanih 32,3 % je naveo da bi to učinio ako će imati pogodnosti i popuste od toga, tako da trgovci imaju o čemu razmišljati, a s obzirom na način plaćanja mobilnim uređajem trgovci bi ponudu svojih proizvoda i usluga mogli reklamirati u stvarnom vremenu korisnicima, ali tu dolazi u pitanje hoće li korisnici te ponude smatrati napornima i dosadnima tijekom vremena. Ovakav način plaćanja čudnim i riskantnim za podatke na mobilnom uređaju smatra 29,2 % ispitanika, tako se i na temelju ovoga odgovora vidi da korisnici nisu još skroz upoznati s ekosustavom mobilnog plaćanja i njegovom sigurnošću.

Prema rezultatima dobivenim istraživanjem provedbom ankete može se zaključiti da su usluge mobilnog plaćanja popularnija kod mlađe populacije korisnika, te da kao zadovoljstvo korištenja ovakvog načina plaćanja korisnici najviše ističu brzinu obavljanja svih potrebnih poslova koji se odnose na plaćanje i sve povezano s njime bez da se čeka u dugim redovima u banci. S obzirom na to da su mladi korisnici skloniji korištenju novih tehnologija i općenito svega što je novo i inovativno pružatelji usluga bi trebali obratiti pažnju na to da korisnicima konstantno nude neke funkcionalnosti kroz aplikaciju ili neka druga rješenja koja ubrzavaju ili nude stalno nešto novo korisnicima, te bi tako podigli kvalitetu svoje aplikacije, a kao produkt

toga povećali bi i zadovoljstvo korisnika. Pružateljima usluga je cilj zadržati korisnike i učiniti ih zadovoljnima kad koriste njihovu uslugu, proizvod ili aplikaciju, jedan od bitnih aspekata jest sigurnost i zaštita korisnika, kroz anketu se vidjelo da dosta korisnika smatra mobilno plaćanje nesigurnim ili su bar skeptični s obzirom na izlaganje osobnih podataka, tako da bi pružatelji usluga (pogotovo aplikacija za plaćanje koje nisu povezane s korisnikovom bankom) trebali staviti više naglaska na to da predstave korisnicima kako je njihova usluga sigurna te na koje su sve načine korisnici zaštićeni kada koriste njihovu uslugu.

7. ZAKLJUČAK

Danas svijet i okruženje u kojem živimo funkcionira tako da se svi poslovi žele obaviti što brže te u što kraćem vremenu i uz što manje napora. Tako korisnici banaka nemaju vremena čekati u dugim redovima po bankama da bi nešto uplatili, isplatili ili samo provjerili stanje računa. Aplikacije za mobilno bankarstvo su omogućile da sve prethodno navedeno bude obavljeno u par klikova i bez fizičkog odlaska u banku. Analizom cjelokupnog ekosustava mobilnog plaćanja opisani su svi sudionici vrijednosnog lanca te važnost svakog pojedinog sudionika za cijeli ekosustav. Kroz istraživanje različitih načina plaćanja mobilnim uređajem vidi se da postoje mnogi sustavi koji se već odavno koriste kao što su SMS plaćanje, QR barcode plaćanja, Internet plaćanja i drugi, ali također postoje tehnologije koje se još trebaju prihvatiti pogotovo u hrvatskoj, kao što su; *Bluetooth* plaćanje, MST plaćanje i plaćanje zvučnim valovima koji predstavljaju zanimljive i inovativne načine i jedan od ciljeva ovoga rada jest da se postojeće aplikacije za mobilno plaćanje nadograde nekim od navedenih načina plaćanja uz postojeće NFC i HCE tehnologije koje već imaju provjerenu kvalitetu.

Istraživanjem provedbom ankete je ustanovljeno da je još dosta korisnika skeptično i u strahu za osobne podatke kad im se spomene mobilno plaćanje. Dokaz tome jest da najviše ispitanika vjeruje aplikacijama mobilnog bankarstva koje su razvile njihove banke razlog tome jest što banke imaju od ranije steknuto povjerenje svojih klijenata. Na pružateljima aplikacijskih usluga je da uvjere klijente da su i druga aplikacijska rješenja sigurna i da korisnici ne moraju biti u strahu kod korištenja drugih aplikacijskih rješenja kao što su Google Pay, Samsung Pay, Pay Pal ili Apple Pay. Kao dokaz prethodno navedenom u radu je opisan proces tokenizacije, zaštite mobilnog novčanika, SSL kriptografija te zaštita cijelog ekosustava mobilnog plaćanja

Na kraju se može zaključiti da pružatelji aplikacijskih usluga i svi uključeni u ekosustav mobilnog plaćanja trebaju ponudom novih usluga, načina plaćanja i tehnologija privući nove korisnike, a isticanjem sigurnosti i zaštite sobnih podataka zadržati povjerenje postojećih korisnika. Iako su mnogi još uvijek skeptični u vezi mobilnog plaćanja, nema sumnje da ova relativno nova tehnologija u Republici Hrvatskoj svakodnevno dobiva nove korisnike. Može se reći da će mobilno i beskontaktno plaćanje uskoro zamijeniti sve dosadašnje načine plaćanja, a zahvaljujući svojoj raznolikosti i mogućnosti primjene mobilnih uređaja, život bez mobilnog plaćanja bit će u budućnosti nezamisliv.

LITERATURA

[1] Academia. Preuzeto sa:

https://www.academia.edu/2563249/Mobile_Payment_Systems_and_Services_An_Introduction [pristupljeno: svibanj 2020.]

[2] White Paper | Mobile Money Mobile Money. Preuzeto sa: http://www.bearingpointabs.com/ [pristupljeno: svibanj 2020.]

[3] Academia. Preuzeto sa: https://squareup.com/guides/mobile-payments [pristupljeno: svibanj 2020.]

[4] Medium. Preuzeto sa: https://medium.com/@appsexpert/a-quick-guide-to-understand-mobile-wallets-and-mobile-payments-5dd932ffdee4 [pristupljeno: svibanj 2020.]

[5] Resarchgate. Preuzeto sa: https://www.researchgate.net/publication/322683076_MOBILE_WALLET-FUNCTIONS_COMPONENTS_AND_ARCHITECTURE [pristupljeno: svibanj 2020.]

[6] Mordorinteligance. Preuzeto sa: https://www.mordorintelligence.com/industry-reports/mobile-payment-market [pristupljeno: svibanj 2020.]

[7] Sammobile. Preuzeto sa: https://www.sammobile.com/samsung-pay [pristupljeno: svibanj 2020.]

[8] Advantio. Preuzeto sa: https://www.advantio.com/blog/mobile-payments-with-digital-wallets-and-tokenization-how-google-pay-apple-pay-and-samsung-pay-protect-your-card-details [pristupljeno: svibanj 2020.]

[9] Babić A, Istraživanje mogućnosti primjene NFC tehnologije u svrhu mobilnog poslovanja, Diplomski rad, Zagreb 2018. [pristupljeno: svibanj 2020.]

[10] Paysafecard. Preuzeto sa: https://www.paysafecard.com/hr-hr/proizvodi/paysafecard/ [pristupljeno: svibanj 2020.]

[11] Mbankcard. Preuzeto sa: https://www.mbankcard.com/bluetooth-mobile-payments/ [pristupljeno: lipanj 2020.]

[12] Linkedin. Preuzeto sa: https://www.linkedin.com/pulse/sound-wave-technology-based-payments-disrupt-low-value-ram-rastogi [pristupljeno: lipanj 2020.]

[13] Diva portal. Preuzet sa: https://www.diva-portal.org/smash/get/diva2:947093/FULLTEXT02 [pristupljeno: lipanj 2020.]

[14] Paypal. Preuzeto sa: https://www.paypal.com/ [pristupljeno: lipanj 2020.]

[15] Nearfieldcommunication. Preuzeto sa: : http://nearfieldcommunication.org/tag-types.html [pristupljeno: lipanj 2020.]

[16] Researchgate. Preuzeto sa: https://www.researchgate.net/publication/262309381_Security_of_the_near_field_communication_protocol_an_overview [pristupljeno: lipanj 2020.]

[17] Eetindija. Preuzeto sa: https://www.eetindia.co.in/using-sound-waves-for-contactless-payments/ [pristupljeno: lipanj 2020.]

[18] Mobiletransactions. Preuzeto sa: https://www.mobiletransaction.org/qr-code-payment-works/ [pristupljeno: lipanj 2020.]

[19] Merchantsavvy. Preuzeto sa: https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/ [pristupljeno: lipanj 2020.]

[20] Codeburst. Preuzeto sa: https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7 [pristupljeno: lipanj 2020.]

[21] Samsung. Preuzeto sa: https://www.samsung.com/us/support/answer/ANS00043932/ [pristupljeno: srpanj 2020.]

[22] Ozdenizci B., Kerem O., Coskun V., A Tokenization-Based Communication Architecture for HCE-Enabled NFC Services. Department of Information Technologies, ISIK University, Turkey 2016.

[23] Googlepay. Preuzeto sa: : https://pay.google.com/about/learn/ [pristupljeno: srpanj 2020.]

[24] Ledecodeur. Preuzeto sa: https://www.ledecodeur.ch/wp-content/uploads/2017/02/WP2016-3-1-4-Mobile-Payments-Security.pdf [pristupljeno: srpanj 2020.]

[25] Enisa, Security of Mobile Payment and Digital Wallets. Preuzeto sa: https://www.enisa.europa.eu/publications/mobile-payments-security [pristupljeno: srpanj 2020.]

[26] Digicert. Preuzeto sa: https://www.digicert.com/ssl-cryptography.htm [pristupljeno: srpanj 2020.]

[27] Autorizirana predavanja: *Ekosustav tržišta informacijsko komunikacijskih usluga*, Fakultet prometnih znanosti, Izvor: https://zir.nsk.hr/islandora/object/fpz%3A1741/datastream/PDF/view

[28] Samsung news. Preuzeto sa: https://news.samsung.com/za/discover-tab-launched-on-samsung-pay [pristupljeno: rujan 2020.]

[29] Academia. Preuzeto sa: https://www.academia.edu/Documents/in/Users [pristupljeno: rujan 2020.]

[30] Autorizirana predavanja: *Sigurnost i zaštita informacijsko-komunikacijskog sustava*, Fakultet prometnih znanosti, Izvor: http://e-student.fpz.hr/ /Predmeti/S/Sigurnost_i_zastita_

POPIS KRATICA

API	(Application Programming Interface) skup aplikacijskih programskih sučelja
BLE	(Bluetooth Low Energy) standard za plaćanje putem mobilnih uređaja uz trošenje manje energije
DOS	(Denial of Service), zloćudni napad uskraćivanjem resursa računalne mreže
EMV	(Europay, MasterCard and Visa) sigurnosni čip za očitavanje podataka s magnetske trake
GDPR	(General Data Protection Regulation*)* opća uredba Eurpske unije o zaštiti osobnih podataka
GPRS	(General Packet Radio Service) paketna, bežična podatkovna komunikacijska usluga
HCE	(Host Card Emulation) razdvaja funkcionalnost emulacije kartice od hardverske SE i pruža virtualni prikaz osjetljivih podataka
ICT	(Information and Communication Technology) produžni pojam za informacijsku tehnologiju koja naglašava ulogu objedinjene komunikacije i integracije telekomunikacija i računala
MST	(Magnetic Secure Transmission) tehnologija mobilnog plaćanja koja za prijenos informacija koristi magnetske valove
MITM	(Man in The Middle) vrsta napada u kojem napadač upada u komunikaciju između klijenta i servera
NFC	(Near Field Communication) tehnologija unutar mobilno ili nekog drugog uređaja pomoću koje se ostvaruje razmjena informacija na kratkim udaljenostima

QR	(Quick Respond) bar kod tip je matričnog barkoda s brzinim čitanjem i velikom pohranom podataka
PAN	(Primary Account Number) broj koji se generira kao jedinstveni identifikator određen za primarni račun
PDA	(Personal Digital Assistant) dlanovnik, digitalni je prijenosni uređaj koji obično stane u dlan
PKI	(Public Key Infrastructure) skup hardvera, softvera, ljudi, politika i postupaka potrebnih za stvaranje, upravljanje, distribuciju, upotrebu, pohranu i opoziv digitalnih potvrda
P2P	(Peer-to-Peer) koncept umrežavanja računala bez poslužitelja, gdje je svako računalo inteligentna radna stanica
SE	(Secure Element) mikroprocesorski čip koji može pohraniti osjetljive podatke i pokrenuti sigurne aplikacije poput plaćanja
SIM	(Subscriber Identity Module) modul na kojem je pohranjen unikatni broj kojim se identificira preplatnik na mobilnoj telefonskoj mreži
SMS	(Short Message Service) usluga slanja kratkih tekstualnih poruka unutar GSM standarda mobilne telefonije
SSL	(Secure Sockets Layer) standardna sigurnosna tehnologija za uspostavljanje šifrirane veze između poslužitelja i klijenta
TR	(Token Request) kratkotrajni token kod kojim klijentski zahtjev odobrava autorizacijski poslužitelj nakon uspješne provjere autentičnosti
TSP	(Token Service Provider) pruža registriranim tražiteljima tokena, primjerice trgovcu koji drži vjerodajnice kartice, tokene za plaćanje
UICC	(Unstructured Supplementary Service Data) komunikacijski protokoli koji GSM mobilni telefoni koriste za komunikaciju

	s računalima operatora mobilne mreže
URL	(Uniform Resource Locator) putanja do određenog sadržaja na Internetu te se obično naziva poveznica, ponekad i mrežna adresa
USSD	(Unstructured Supplementary Service Data) nestrukturirani podaci o dodatnim uslugama, koji se ponekad nazivaju i brzi kodovi ili kodovi značajki
WAP	(Wireless Application Protocol) tehnički standard za pristup informacijama putem mobilne bežične mreže. WAP preglednik je web preglednik za mobilne uređaje poput mobilnih telefona koji koriste protokol

POPIS SLIKA

Slika 1: Prikaz naglog porasta broja mobilnih transakcija u milijardama dolara 3
Slika 2: Prikaz beskontaktnog plaćanja na POS uređaju putem mobilnog uređaja 4
Slika 3: Dijagram zahtjeva za izradu tokena za plaćanje 7
Slika 4: Standardni format slanja SMS poruke za plaćanje usluge 11
Slika 5: Prikaz 3 jednostavna koraka prilikom plaćanja paysafecard PIN kodom 13
Slika 6: Plaćanje BLE tehnologijom 15
Slika 7: Sigurni tijek transakcije ToneTag 16
Slika 8: Prikaz klizanja karata MST u Samsung Payu 17
Slika 9: Prikaz plaćanja QR kodom 18
Slika 10: NFC emulacija kartice 21
Slika 11: Emulacija kartice sa sigurnosnim.....21
Slika 12: HCE komunikacijski tijek.....24
Slika 13: Prikaz potražnje i ponude u ICT vrijednosnom lancu 26
Slika 15: Primjer funkcioniranja gateway poslužitelja 31
Slika 16: Sekvencijalni dijagram Apple Pay platnog procesa 33
Slika 17: Prikaz korištenja Samsung Pay aplikacije u 3 jednostavna koraka.....36
Slika 18: Prikaz sudionika Google Pay ekosustava 36
Slika 19: Lanac vrijednosti mobilnog plaćanja 41
Slika 20: Prikaz uključivanja mobilnog operatora u lanac vrijednosti mobilnog plaćanja 42
Slika 21: Slika prikazuje kako funkcionira PayPal aplikacija 45
Slika 22: Odnosi između uzroka prijetnje, prijetnje i osnovnih načela.....53

POPIS GRAFIKONA

Grafikon 1: Raspon godina ispitanika 58
Grafikon 2: Završeni stupanj obrazovanja ispitanika 59
Grafikon 3: Prikaz koliko često korisnici koriste uređaj u danu 59
Grafikon 4: Koliko često ispitanici koriste mobilni uređaj za plaćanje.....60
Grafikon 5: Koji oblik plaćanja korisnici najviše koriste 61
Grafikon 6: Prikazuje koliko ispitanici smatraju mobilno plaćanje sigurnim.....62
Grafikon 7: Prikazuje koju banku ispitanici koriste.....63
Grafikon 8: Prikaz kako ispitanici ocjenjuju aplikaciju mobilnog bankarstva svoje banke 63
Grafikon 9: Prikazuje što najviše korisnici vole kod usluga mobilnog plaćanja 64
Grafikon 10: Prikaz koliko ispitanika posjeduje NFC tehnologiju 65
Grafikon 11: Prikaz jesu li korisnici spremni koristiti mobilni uređaj za beskontaktno plaćanje66

POPIS TABLICA

Tablica 1: Prikaz sudionika lanca vrijednosti plaćanja kreditnom karticom.....40

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Analiza ekosustava mobilnog plaćanja**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 16-09-20

Student/ica:
Zdravko Gospočić
(potpis)