Analiza korisničkog iskustva primjene telekomunikacijskih usluga u funkciji elektroničke naplate

Mađerić, Toni

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:563164

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Toni Mađerić

ANALIZA KORISNIČKOG ISKUSTVA PRIMJENE TELEKOMUNIKACIJSKIH USLUGA U FUNKCIJI ELEKTRONIČKE NAPLATE

DIPLOMSKI RAD

Zagreb, 2015.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA KORISNIČKOG ISKUSTVA PRIMJENE TELEKOMUNIKACIJSKIH USLUGA U FUNKCIJI ELEKTRONIČKE NAPLATE

ANALYSIS OF THE USER EXPERIENCE OF USING TELECOMMUNICATIONS SERVICES IN ELECTRONIC BILLING

Mentor: Prof. dr. sc. Dragan Peraković

Student: Toni Mađerić, 0269022120

Zagreb, 2015.

Sažetak

Elektronička naplata je primjena informacijskih i komunikacijskih tehnologija kao podrška svim poslovnim aktivnostima. Elektronička trgovina je vrsta elektroničkog poslovanja u kojem se transakcije provode preko Interneta. Svrha ovog istraživanja je analizirati korisničko iskustvo korištenjem telekomunikacijskih usluga u funkciji elektroničke naplate i pojasniti vrste i značaj sustava elektroničke naplate. Cilj ovog istraživanja je doznati koji način naplate korisnicima najviše odgovara, istražiti koju vrstu elektroničke naplate korisnici najviše koriste i da li su spremni prijeći na neki novi i moderniji oblik naplate. Istaknuti će se važnost elektroničkog novca u poslovanju uz sigurnosne značajke, te sustave zaštite elektroničkog plaćanja. Analizirat će se platforma „Google Wallet“ i postojeća arhitektura iste, te prednosti svakodnevne primjene ove usluge. Istražit će se mogućnost korištenja mobilnog terminalnog uređaja na bankomatima, blagajnama, te ostalim uređajima koji zahtijevaju identifikaciju i naplatu, te primjena u svakodnevnom životu korisnika.

KLJUČNE RIJEČI: korisničko iskustvo; analiza; korištenje telekomunikacijskih usluga; elektronička naplata; elektronički novčanik

Summary

Electronic payment is the application of information and communication technologies to support all business activities. Electronic commerce is a type of electronic business in which transactions are conducted over the Internet. The purpose of this research is to analyse the user experience by using telecommunications services in the function of electronic billing and clarify the types and importance of electronic billing. The aim of this research is to find out which billing method are the most convenient for the users. Explore what kind of electronic billing is most used by the users and if they are willing to switch to a new and modern form of payment. The importance of electronic money in the business and protection systems of electronic money with security features will be highlighted. The platform „Google Wallet“ and the existing architecture of the same will be analyzed, and the benefits of daily application of this service. The possibility of using the mobile terminal device at ATMs, cash registers will be investigate, and other devices that require the identification and payment, and application in daily life of users.

KEYWORD: user experience; analysis; the usage of telecommunications services; electronic payment; electronic wallet

SADRŽAJ

1. Uvod 1

2. Evolucija usluga elektroničke naplate 3

2.1. Evolucija Internet mreža 4

2.2. Povijest sustava naplate preko elektroničkih kartica 7

2.3. Razvoj i napredak bežične tehnologije za naplatu 10

2.4. Primjena biometrijske tehnologije u svrhu naplate 12

3. Sustavi plaćanja elektroničkim novcem i sigurnosne značajke 15

3.1. Elektronički novčani sustavi 16

3.1.1. Notacijski sustavi 16

3.1.2. Simbolički sustavi 17

3.1.3. Centralizirani sustavi 18

3.1.4. Decentralizirani sustavi 18

3.2. Primjena elektroničkog novca 19

3.3. Trendovi elektroničkog novca 21

3.4. Sigurnosni aspekti elektroničkog novca 25

3.3.1. Preventivne mjere 27

3.3.2. Mjere detekcije 31

3.3.3. Mjere za suzbijanje 32

4. Značajke i arhitektura platforme Google Wallet 33

4.1. Zaštita od prijevare 36

4.2. Sigurnosni aspekti 37

4.3 Osnovno korištenje aplikacije 39

4.4. Dodatne značajke i funkcionalnosti 42

4.5. Arhitektura Google Wallet platforme 44

5. Analiza korisničkog iskustva korištenja usluga elektroničkog plaćanja 50

6. Zaključak 66

LITERATURA 68

POPIS SLIKA 74

POPIS GRAFIKONA 76

PRILOG DIPLOMSKOG RADA 78

1. Uvod

U ranim 1990-im godinama poslovni i potrošački svijet je naišao na novi način poslovanja, koji je nazvan elektroničko plaćanje. Tijekom godina elektroničko poslovanje je postalo popularan i poznat način provođenja plaćanja. Popularnost i trend telekomunikacijskih usluga elektroničkog plaćanja u svijetu je danas u stalnom rastu, te postaje sve sigurniji način poslovanja. Korisnicima olakšava plaćanje i donosi znatnu uštedu vremena i novca.

Uspjesi poslovnih web mjesta doveli su do stvaranja novog koncepta poslovanja, tj. koncepta elektroničkog poslovanja. U početku se on ostvarivao samo u obliku elektroničkog kataloga gdje su tvrtke objavljivale informacije o proizvodima i uslugama koje su nudile potrošačima. S vremenom su počeli dodavati brojne nove usluge kao što su mogućnost jednostavnog pretraživanja ponude (navigacija po *web* mjestu), dogovaranja uvjeta kupnje i isporuke, naručivanja proizvoda ili usluga, elektroničkog plaćanja te isporuke dobara koje je moguće digitalizirati (glazba, igre, knjige, video, itd.). Porastom broja poslovnih web mjesta razvijaju se internetska (elektronička) tržišta na kojima vlada sve veća konkurencija među tvrtkama koje se putem svojih web mjesta uključuju u tržišne tokove. Ukratko opisan razvoj elektroničkog poslovanja odvijao se vrlo velikom brzinom, točnije manje od jednog desetljeća.

Elektroničko poslovanje je doživjelo veliku popularnost, povećavao se broj tvrtki koje su svoje poslovanje zasnivale na korištenju internetske tehnologije. Vrijednost tih kompanija je naglo rasla ali i broj klijenata (povećavalo se povjerenje javnosti o takvom poslovanju). Ubrzo je došlo i do prvih poteškoća u elektroničkom poslovanju. Mnoge tvrtke su ušle u elektroničko poslovanje bez dobro razrađenih modela i klijentima su nudili obećanja koja nisu mogli ispuniti. Iz pogrešaka su izvučene pouke i lekcije koje se više ne smiju ponoviti. Tvrtke koje su opstale prionule su analizi svojih postupaka i temeljito su razradile svoje nove poslovne modele. Od tada elektroničko poslovanje bilježi uspjehe, a ono se mora voditi u skladu s općim ekonomskim zakonitostima.

Danas se nove tehnologije često nađu na temi kritika i nepovjerenja, pogotovo kad je riječ o elektroničkoj naplati. Relativno malo broj korisnika se usudi svoj novac predati aplikaciji i ima povjerenja u sigurnost same aplikacije. Elektronička naplata, iako pojednostavljuje sam proces kupnje i naplate, često je na meti raznih hakera, aplikacija koje traže ranjivosti da bi ih iskoristile. Aplikacije poput Google Wallet - a se svakim danom sve više sigurnosno razvijaju, ne bi li postale otporne na hakerske napade.

Iako korištenje usluge elektroničke trgovine čini život jednostavnijim, u Republici Hrvatskoj se ne koristi dovoljno. Prema podacima GFK[1] – a, u prosjeku korisnici u Republici Hrvatskoj nisu previše tehnološki opremljeni, ali ipak prate sve zapadne trendove. Korisnici su još uvijek skeptični prema telekomunikacijskim uslugama elektroničke trgovine, a glavni razlog je sigurnost. Korisnike treba educirati, te im pokazati da su forme na Internetu zaštićene. Može se očekivati, kada se promijeni percepcija korisnika da elektronička trgovina može uštedjeti vrijeme i novac, te se postotak građana koji koriste usluge elektroničkog plaćanja u RH može približiti svjetskim brojkama.

Svrha ovog istraživanja je analizirati korisničko iskustvo korištenjem telekomunikacijskih usluga u funkciji elektroničke naplate i pojasniti vrste i značaj sustava elektroničke naplate. Cilj ovog istraživanja je doznati koji način naplate korisnicima najviše odgovara, istražiti koju vrstu elektroničke naplate korisnici najviše koriste i da li su spremni prijeći na neki novi i moderniji oblik naplate.

Naslov diplomskog rada je: Analiza korisničkog iskustva primjene telekomunikacijskih usluga u funkciji elektroničke naplate. Rad je podijeljen u šest cjelina:

1. Uvod
2. Evolucija usluga elektroničke naplate
3. Sustavi plaćanja elektroničkim novcem i sigurnosne značajke
4. Značajke i arhitektura platforme Google Wallet
5. Analiza korisničkog iskustva korištenja usluga elektroničkog plaćanja
6. Zaključak

U drugom poglavlju je opisana evolucija usluga elektroničke naplate od samih početaka Interneta do današnjih modernih tehnologija.

Treće poglavlje sadrži opis značajka sustava elektroničkog novca, te njegove primjene u poslovanju, uz sigurnosne značajke. Opisani su i podijeljeni elektronički novčani sustavi uz rezultate istraživanja, kao i trendovi elektroničkog novca koji su danas aktualni. Definirani su sigurnosni aspekti elektroničkog novca uz preventivne mjere, mjere za suzbijanje i mjere detekcije.

U četvrtom poglavlju se opisuju značajke platforme Google Wallet, te analiza postojeće arhitekture iste.

U petom poglavlju je prikazana analiza rezultata anketnog upitnika. Anketni upitnik sadrži podatke o korisničkom iskustvu korištenja usluga elektroničke naplate.

[1] **GFK** – Centar za istraživanje tržišta d.o.o. Zagreb

2. Evolucija usluga elektroničke naplate

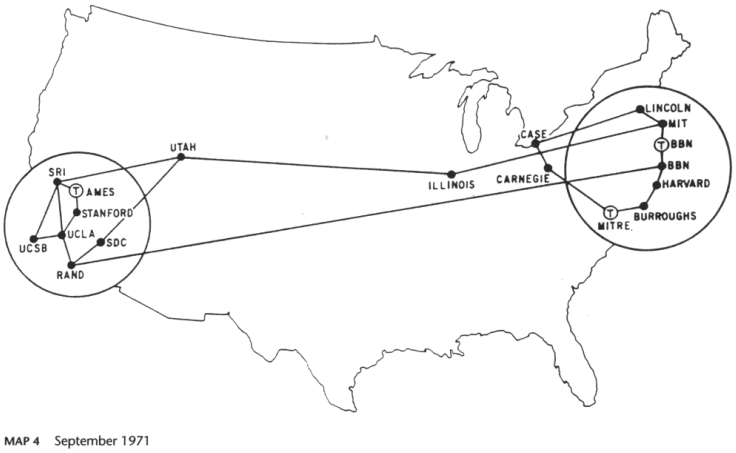
Razvojem Interneta razvio se novi i učinkoviti način naplate zvan elektronička naplata. Početkom 60. Godina 20. stoljeća američki su znanstvenici predvidjeli međusobno spojen veći broj računala pomoću kojih će svatko moći pristupiti podacima i programima s bilo kojeg mjesta. Povezivanjem dvaju računala smještenim na različitim američkim sveučilištima vezom preko telefonske linije, znanstvenici su stvorili prvu svjetsku računalnu mrežu WAN[2]. S tim eksperimentom su dokazali da računala mogu komunicirati, pokretati programe i pronaći podatke na udaljenom računalu, [22].

Kroz povijest, metode naplate su se mijenjale kontinuirano zbog prirodnih sklonosti ljudi da istražuju i razvijaju pragmatična rješenja kroz korištenje raspoloživih resursa. Novi oblici tehnologije poboljšavaju učinkovitost i jednostavnost ostvarenja ciljeva, te stvaranje vrijednosti. Metoda stvaranja elektroničke kupnje je moderna praktičnost i standard za većinu poduzeća danas. Elektronička plaćanja nude fleksibilnost za potrošače koji ne nose gotovinu ili kupuju na mreži. Ljudi širom svijeta iskorištavaju trend metode gdje usvajaju sustav naplate za stvari koje žele i trebaju. Inovacija služi kao prirodna sklonost za razvojem i korištenjem sustava za ostvarenje rješenja za svakodnevne zadatke. Razvoj elektroničkih sustava naplate slijedi dostupnu tehnologiju, koja može ostvariti željeni ishod prihvaćanja valute u zamjenu za robu, [22].

[2] **WAN** – Wide Area Network

2.1. Evolucija Internet mreža

1969. godine znanstveno istraživački tim ARPA[3] započeo je izgradnju prve računalne mreže ARPANET. Budući da je mreža ARPANET rasla, ARPA i njezini suradnici nisu završili sa svojim istraživanjima. Okrenuli su se istraživanju satelitskih i pokretnih paketnih radio mreža te dokazali da postojeći ARPANET – ovi protokoli nisu dovoljno dobri za uporabu ako se koristi velik broj mreža. Zato je osmišljena nova varijanta protokola TCP[4] kojim se može kontrolirati komunikacija između više manjih mreža. Kasnije je protokol TCP podijeljen na više protokola (TCP i IP) koji se i danas koriste. U TCP/IP protokole svrstava se i protokol za prijenos datoteka FTP[5]. S vremenom je ovakav sustav mreže nazvan Internetom.



Slika 2.1. Prikaz početka ARPANET mreže, [41].

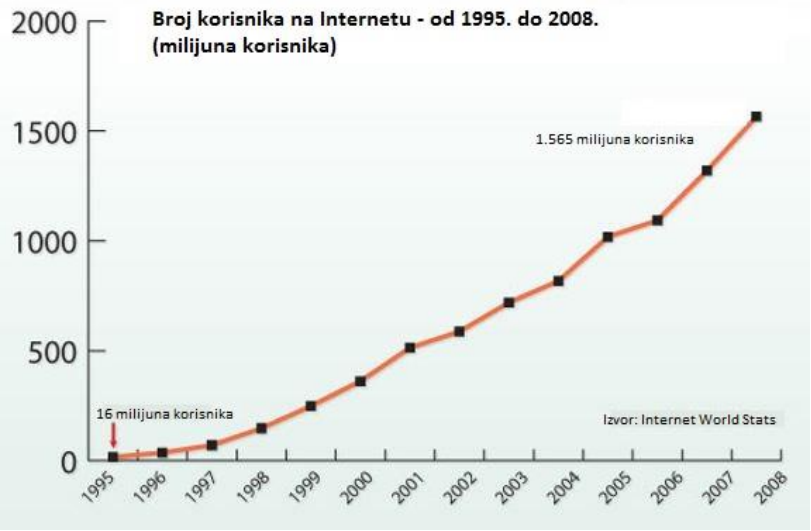
1984. godine američki istraživači Nacionalne zaklade za znanost (NSF)[6] započeli su izgradnju nasljednika ARPANET – a koji bi omogućio brzi prijenos podataka preko mreže te bio pristupačan svim Sveučilištima, istraživačkim laboratorijima, knjižnicama i muzejima. Izgradili su osnovicu svih mreža kojom su povezali šest velikih računalnih centara. Mreža je nazvana NSFNET i sastojala se od superračunala smještenih u različitim računalnim centrima, te od mikroračunala koja su činila pod mrežu, [22].

[3] **ARPA** – Advanced Research Project Agency
[4] **TCP** – Trasport Control Protocol
[5] **FTP** – File Transport Protocol
[6] **NSF –** National Science Fundation

NSFNET je bila spojena na ARPANET i koristila istu tehnologiju, međutim za razliku od ARPANET – a od samog početka je koristio TCP/IP i stoga se može nazvati prvom globalnom TCP/IP mrežom.

Zbog velikog porasta malih mreža, koje su se spajale na ARPANET, traženje slobodnog središnjeg mrežnog računala postalo je vrlo skupo. Zato je tijekom 80-ih godina kreiran sustav kojim se računala organiziraju prema domenama i definiraju imena koja odgovaraju određenoj IP adresi. Takav sustav je nazvan sustav naziva za područja (DNS[7]).

Do 1989. godine broj središnjih mrežnih računala spojenih na mrežu prešao je 100 000 te je sve veći i broj korisnika iz obrazovnih, vladinih i vojnih institucija koji koriste internetske servise. Ujedno, potaknuti novom tehnologijom tj. jeftinijim računalima manjih dimenzija, početkom 1990-ih Internet postaje dostupan svim ljudima tj. budućim korisnicima Interneta koji su se mogli spojiti na Internet iz svoje kućne fotelje. Zbog sve većeg broja korisnika i umreženih računala, fizičar Tim Berners-Lee razvio je 1991. godine novi internetski servis pod nazivom WWW[8] ili web koji je koristio poveznice i grafičko sučelje razumljivo korisnicima, [22].

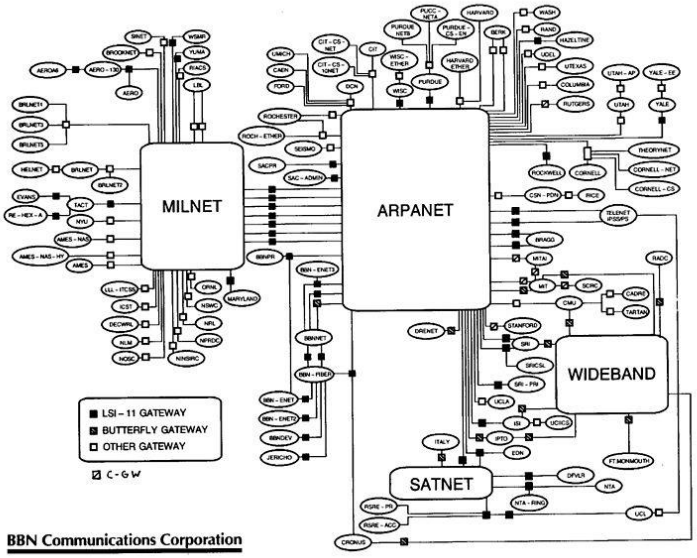


Slika 2.2. Rast uporabe Interneta kroz godine, [42].

[7] **DNS** – Domain Naming System
[8] **WWW** – World Wide Web

Izraz Internet je posvojen u RFC[9] – u izdanom na TCP protokolu (RFC 675), te je bila kratica pojma umrežavanja. Općenito, Internet je bila bilo koja mreža koja koristi TCP/IP. Bilo je to vrijeme kad je ARPANET bio povezan s NSFNET – om u kasnim 80-im. Taj pojam je bio korišten kao naziv mreže, kao velika i globalna TCP/IP mreža. Kako je interes za umrežavanje rastao i nove se aplikacije razvijale, Internet tehnologije su se proširile po ostatku svijeta. Pristup mreži preko TCP/IP – a je značio jednostavnost za korištenje bilo koje mrežne infrastrukture, kao što je IPSS X.25 mreža za prijenos Internet prometa.

Tehnologije usmjeravanja su s vremenom razvijale da bi uklonile preostale centralizirane aspekte usmjeravanja. EGP[10] je bio zamijenjen novim BGP[11] protokolom. To je osiguralo mrežnu topologiju za Internet i smanjilo centraliziranu arhitekturu koju je ARPANET istaknuo. Godine 1994. predstavljen je CIDR[12] da bi podržao bolje očuvanje adresnog prostora, što je omogućilo korištenje agregacije rute i smanjenje veličine tablice usmjeravanja, [2].



Slika 2.3. TCP/IP Internet karta iz 1986. godine, [43].

[9] **RFC** – Request for comments
[10] **EGP** – Exterior Gateway Protocol
[11] **BGP** – Border Gateway Protocol
[12] **CIDR** – Classless Inter-Domain Routing

2.2. Povijest sustava naplate preko elektroničkih kartica

Ideja naplate preko kartica pojavila se prije više od 125 godina, u dalekoj 1880. godini. Tada je poznati američki znanstvenik Edward Bellamy u svojoj knjizi „Pogled unatrag“, u kojoj je predložio korištenje „*prepaid*“ kartica. Međutim, njegova obećavajuća ideja je propala, te je tek nakon četvrtine stoljeća (1914.) bio prvi pokušaj da se koriste kreditne kartice, no ubrzo je i to promašeno. Više od 35 sljedećih godina se ništa nije dogodilo s idejom elektroničkog načina plaćanja, [3].

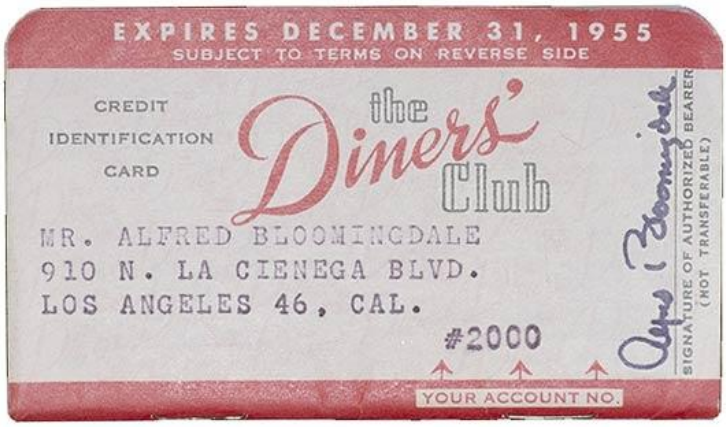
Godine 1950. Diners Club International (IDC) je izdao prve svjetske univerzalne platne kartice „Diners Club“. Nakon toga, sljedeće godine „Franklin National Bank“ je izdala prve kreditne kartice. Sedam godina kasnije „Bank of America“, tada najveća američka banka u zemlji je izdala prvu univerzalnu bankovnu karticu koja je danas poznata pod nazivom „Visa“. Već 1965. godine je formirana prva udruga bankovnih kartica pod nazivom „Eurocard International“. Ozbiljan konkurent Visa – i se pojavio osam godina kasnije, 1965. godine. Sve poveće banke u Californiji su počele izdavati „Master Charge“, kasnije nazvanu „Master Card“. U to vrijeme je nastajao uvodna faza povijesti elektroničkog plaćanja, sljedeće razdoblje je bilo povezano s razvojem informacijskih tehnologija te njihovih primjena u bankarstvu, [3].

Druga polovica dvadesetog stoljeća bila je poznata po brzom razvoju informacijskih tehnologija u cjelini, te dio mikrotehnologija. Američke banke su po prvi put u svijetu počeli primjenjivati elektroničke metode prijenosa novca. Tehnologije elektroničkog prijenosa, kao što su bile EFT[13] su se pojavile. Godine 1968., svijet je ugledao tehnologiju razmijene elektroničkih podataka EDI[14], koja je kasnije postala osnova za elektroničke transakcije, [4].

[13] **EFT** – Eletronic Funds Transfer
[14] **EDI** – Electronic Data Interchange

Elektronička plaćanja su se aktivno razvijala, svijet je počeo koristiti kreditne kartice s dovoljno povjerenja. Godina 1974. je bila prekretna točka u pogledu razvoja elektroničkom plaćanja u SAD – u. To je bilo vrijeme kad je Robert Moreno u Francuskoj registrirao patent za proizvodnju tehnologije za pametne kartice. U SAD – u se godinu kasnije proizveo ATM[15] (bankomat) za podizanje novca bez čekanja u redu. Razvoj informacijskih tehnologija nije mirovao, te su se 1979. godine elektronički terminali za bezgotovinska bankovna plaćanja (EFTPOS[16]) prvi puta počeli koristiti u SAD – u, [7].

Već 1984. godine, poduzeća financijskog sektora su počela aktivno koristiti e-poštu za komunikaciju s klijentima. To je bio prvi korak na putu do elektronskog bankarstva i Internet bankarstva. Trebalo je još tri godine da za prve banke koje su pružale usluge na Internetu, [7].



Slika 2.4. Primjer prve Diners Club kreditne kartice, [44].

Godine 1971. je stvoreno prvo klasično računalo (IBM PC) i razvoj mikroelektronike je u tom trenutku skočio. U drugoj polovici 80. – ih godina, mikroprocesor je uspješno instaliran u plastične kreditne kartice, što je predodredilo pojavu nove vrste novca – digitalnog novca. U povijesti elektroničkog novca revolucionarna godina je bila 1993., kada je Dr. David Chaum (voditelj kriptografije u civilnom ratu) razvio softversko rješenje – eCash tehnologiju za rad s digitalnim novcem, [4].

[15] **ATM** – Automatic Teller Machine
[16] **EFTPOS** – Electronic Founds Transfer at Point Of Sale

Kreditne kartice su postale osnovni i neizbježni dio današnjeg društva. Jedan su od primarnih oblika za izvršavanje transakcije u većini maloprodajnih poduzeća. Kako je obrada kreditnih kartica postala sve složenija, vanjske uslužne tvrtke su počele prodavati usluge članovima udruge Vise i MasterCard – a. To je smanjivalo troškove programa banaka za izdavanje kartica, plaćanje trgovaca i podmirenje računa korisnika, omogućavajući veću ekspanziju industrije plaćanja.

Visa i MasterCard su razvili pravila i standardizirane postupke za rukovanje protokom bankovnih kartica kako bi se smanjila prijevara i zloupotreba kartica. Također su proizveli međunarodne sustave obrade za rukovanje razmjenom novca i informacija, te arbitražno rješavanje sporova između članova. Iako je American Express bio među prvim tvrtkama koje su izdavale platne kartice, to nije bio do 1987. godine kada su izdali kreditnu karticu koja je omogućavala korisnicima da platu preko vremena, nego na kraju svakog mjeseca. Taj izvorni poslovni model je bio usmjeren na putne i zabavne troškove od strane poslovnih ljudi, koji je uključivao značajan prihod od trgovaca i godišnje članarine od korisnika, [5].

Još jedan nedavni ulazak u kartično poslovanje je bio „Discover Card“, originalno dio Sears Corporations-a. Prema Discover-u, njihova prva kartica je predstavljena na Super Bowl-u 1986. godine. Usluge Discover Card-a su nastojale stvoriti novi brend s vlastitom trgovačkom mrežom, te tvrtka je bila uspješna u razvoju trgovačkog prihvaćanja. Sudska presuda nepovjerenja protiv Visa-e i MasterCard-a 2004. godine, koja je bila pokrenuta od strane Američke vlade i Ministarstva Pravosuđa, promijenila je odnos Visa-e i MasterCard-a sa bankama. To je omogućilo bankama i drugim izdavateljima kartica pružiti klijentima usluge American Express-a i Discover Card-a, [5].



Slika 2.5. Primjer Discover Card – a, [45].

2.3. Razvoj i napredak bežične tehnologije za naplatu

Evolucijom elektroničkih tehnologija za naplatu se došlo do spoznaja novih tehnologija koje su doprinijele nove načine naplate. Razvoj kreditnih kartica je bio novi korak prema modernijim načinima naplate, te je „otvorio vrata“ novim tehnologijama.

Prvi primjer naplate preko mobilnog uređaja potječe iz 1997. godine kad je Coca Cola predstavila ograničen broj automata gdje su korisnici mogli obaviti plaćanje. Korisnik je slao tekstualnu poruku automatu za namještanje naplate i automat bi potom izbacio proizvod. Mobilna plaćanja su se prvi put pojavila 1997. godine preko tzv. „Merita banke“ koja je omogućavala tekstualne poruke u svrhu izvršenja naplate, [7].

Bilo koji uređaj koji omogućuje naplatu korištenjem radio-frekvencijske identifikacije RFID tehnologije koristi bežičnu tehnologiju. Antena i instalirani čip omogućuju kupcu da s običnim pokretom uređaja preko čitača kartica izvede kupnju željenog proizvoda. Sigurnost bežičnog plaćanja je ista kao i za kreditne kartice. Koriste se zakoni za zaštitu od prijevara, te sigurnosni kanali i enkripcija su podržani prilikom slanja informacije o kreditnoj kartici i PIN brojevima. Za kupnju proizvoda s visokim cijenama ili nekoliko kupnji u kratkom vremenskom periodu, od korisnika se traži da manualno unese PIN da bi se osiguralo od krađe. Obično bežična naplata je brža zato što ne zahtijeva PIN ili potpis, dok isto tako može izazvati da korisnik potroši više novaca jer kupuje brzo i lako, [7].

Tako se krajem 90-ih počele razvijati nove tehnologije tzv. bežične tehnologije koje su bili ključne za elektroničku naplatu tog doba. Razvijao se NFC[17], bežična tehnologija koja je omogućavala komunikaciju na kratkim udaljenostima. NFC potječe od RFID tehnologije, odnosno podskup je RFID – a s kraćim rasponom (dometom) komunikacije zbog sigurnosnih razloga. Godine 2004. Nokia, Sony i Phillips su osnovali NFC forum, u kojem su zagovarali na promociju sigurnosti, jednostavnost korištenja i popularnost NFC tehnologije. Godine 2006. su razvili prvi set značajki za NFC tagove, a radi se o malim objektima koji sadržavaju informacije koje kompatibilni uređaji (pametni telefon) mogu registrirati, te pročitati informacije. Informacija na tagu je obično *read-only*[18] karaktera, dok neki tagovi omogućuju čitanje i upisivanje novih informacija ili izmjena starih, [8].

[17] **NFC** – Near Field Communication – tehnologija kratkog dometa bežične komunikacije
[18] **Read-only** – informacije koje se mogu samo pročitati (očitati), bez mogućnosti promijene

Prvi NFC kompatibilni mobilni uređaj je bio Nokia 6131, promijenjen tijekom vremena. Kako su godine prolazile, sve više specifikacija se ugrađivalo za elektronsku naplatu, dijeljenje video sadržaja, linkova i igara između pametnih mobilnih uređaja i drugih NFC uređaja. Android je proizveo prvi NFC mobilni uređaj, Samsung Nexus S, 2010. godine. Danas tržište NFC-a je među dominantnima u Europi, Aziji i Japanu, dok SAD je također viđen znatan rast u tom području. Procijenjeno je da će NFC uskoro evoluirati u popularni oblik naplate i tehnologiji razmijene podataka u SAD – u, [8].

Prvi primjer bežične naplate potječe u obliku SpeedPass[19]-a 1997. godine. Stanice Mobil-ove pumpe su nudile uređaje za bežično plaćanje. Korisnik bi na benzinskoj pumpi prošao mobilnim uređajem preko označenog kvadrata, te bi gotovo trenutno izvršio naplatu. Danas ExxonMobil još nudi tu uslugu, te ostale benzinske pumpe imaju udružene tehnologije bežične naplate za svoje izbore plaćanja, [7].



Slika 2.6. Bežična naplata, [46].

S tim mogućnostima naplate, te kasnije naplatom preko mobilnog uređaja koji podržava NFC, korisnik može pohraniti više kreditnih kartica i ostalih metoda naplate u jedan mobilni uređaj. Nudeći visoku razinu kompatibilnosti za različite kompanije i tehnologije, NFC može evoluirati u jednostavnu metodu naplate u jednom koraku koja funkcionira svugdje gdje korisnik želi izvršiti kupnju.

[19] SpeedPass – bežična naplata na benzinskoj pumpi

2.4. Primjena biometrijske tehnologije u svrhu naplate

Biometrijska naplata je POS[20] tehnologija koja koristi biometrijsku autentifikaciju identificiranje korisnika i autorizacija za oduzimanje sredstava s bankovnog računa. Naplata preko otiska, baziranja na očitanju otiska prsta je najčešća metoda biometrijske naplate. Često, sustav koristi autentifikaciju preko dva faktora, u kojoj skeniranje prsta zamjenjuje provlačenje kartice i utipkavanje PIN-a, [9].

Primjer obavljanja kupnje preko očitavanja otiska prsta po fazama:

- Kupac registrira biometrijski program u trgovini prezentirajući valjanu identifikaciju i informaciju računa banke.
- Kupac skenira otisak prsta koristeći se čitačem za otiske.
- Čitač otiska prstiju enkriptira više „*pont-to-point"* mjerenja otiska prsta i pohranjuje korisnikove biometrijske podatke u centraliziranu bazu podataka.
- Kupac sad ima opciju uzimanja biometrijskih plaćanja na POS registru. Ako odabere biometrijsku naplatu, samo skenira svoj prst na blagajni s čitačem i unese svoj identifikacijski broj.
- Elektronički čitač uspoređuje podatke od novog skeniranja sa kriptiranim podacima u bazi podataka, te potom dopušta ili odbija transakciju. Ako dopušta, sredstva s računa se elektronički prenose od računa kupca prema trgovcu, [9].

U SAD-u, biometrijsko plaćanje je povećalo popularnost u trgovinama, benzinskim pumpama, te na mnogo drugih mjesta. Godine 2006. „Pay By Touch", vodeći pružatelj biometrijske naplate je izvijestio da više od dva milijuna korisnika je upisano u biometrijske usluge i da je „Pay By Touch" autentificirao približno 8 bilijuna američkih dolara u transakcijama, [9].

[20] **POS** – Point Of Sale

Prednosti biometrijske naplate obuhvaćaju:

- Poboljšana sigurnost za krajnjeg korisnika.
- Brze transakcije.
- Nema potrebe za nošenjem gotovine, čekova i kreditnih kartica.
- Manji troškovi po transakciji za trgovca, uspoređujući s porezima standardnih debitnih ili kreditnih kartica, [9].

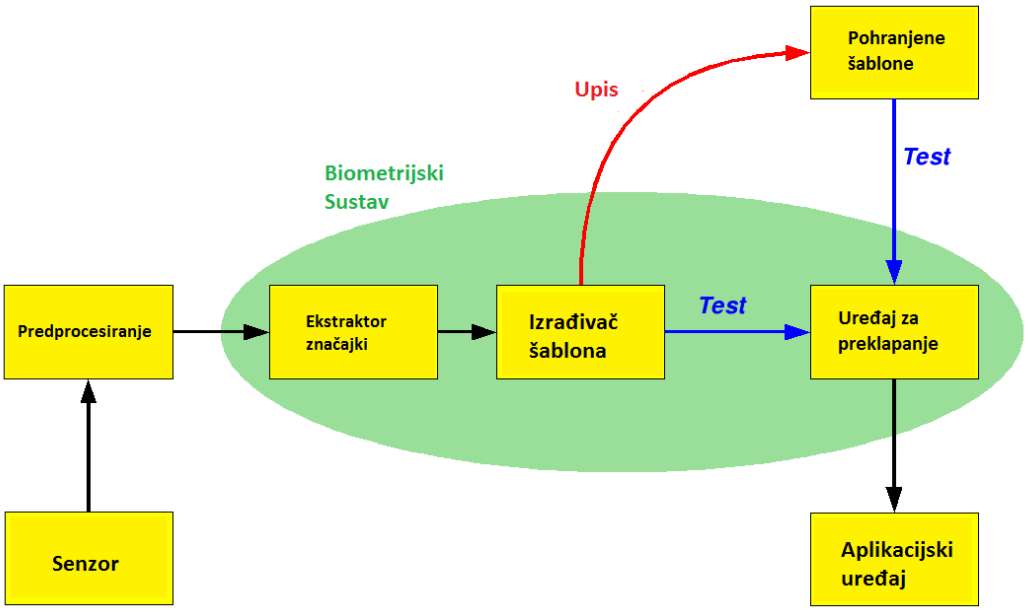


Slika 2.7. Naplata očitanjem otiska prsta, [47].

Biometrijska naplata je danas sporna. Tradicionalno, otisci prstiju su uvijek bili povezani s policijom. Kritičari za biometrijska plaćanja se boje da otisci prstiju mogu biti dostupni vladinim agencijama ili policijskim službenicima. Pružatelji usluga biometrijske naplate se brzo ukažu da oni ne čuvaju korisnikove stvarne otiske prsta u njihovim bazama podataka. Čuvaju samo kriptirani broj izveden iz mjera skeniranjem prsta. Taj broj služi za identifikaciju korisnika, ali ne i otiska prsta. U konačnoj analizi, sustav biometrijske naplate, kao bilo koji sustav koji ima pristup osjetljivim informacijama, je siguran kao povezane baze podataka i transakcije, [9]. Biometrija kao tehnologija se već se dulje koristi u bankama diljem svijeta. Najčešće se koriste otisak prsta, potpis, geometrija ruke te prepoznavanje lica i glasa. Svi sustavi su postavljeni u svrhu evidencije radnog vremena, kontrole pristupa, sigurnosti transakcija, te sigurnosti baza i mreža. Ozbiljan rast primjene biometrije u svijetu bilježi se početkom 21. stoljeća. U Hrvatskoj se ovakav sustav počeo primjenjivati u svrhu evidenciju radnog vremena, te tada je bio prvi u Europi, [10].

Sustav biometrijske naplate može biti troškovno efektivan, jer omogućuje prihvaćanje i izvršavanje naplate bez ikakve potrebe za provlačenjem kartice ili unošenjem PIN broja. Kad se primijetilo da je biometrija kompletno jedinstvena za svaku osobu, ova metoda komercijalnog sustava naplate je generalno prepoznatljiva kao mnogo lakša i dosta pristupačna za one koje koriste ovu tehnologiju. Očito je više rada koje je potrebno za napraviti naplatu korištenjem biometrijske identifikacijske verifikacije da bi se lakše koristila, ali se dokazuje da će postati nešto što će biti mnogo popularno, [11].

Ovaj način naplate uključuje zamjenu provlačenja kreditne kartice i PIN sustava, te se sve procedure vrše s biometrijskim čitačem. Svrha uređaja za biometrijsko skeniranje je pojednostavniti proces biometrijske autentifikacije, te se vjeruje da će biti puno sigurnije nego korištenje kreditne kartice i PIN broja. U biometrijskom bankarstvu, prva stvar koja se dogodi u procesu kupnje je da se kupac registrira na jedno biometrijsko naplatno rješenje koje su trenutno dostupne u različitim trgovinama i kioscima u svijetu. Kupac mora predočiti valjanu osobnu, broj bankovnog računa i dati otiske prsta na skeniranje. Sve ove informacije se potom spremaju na računala, te mogu biti trenutno dostupna kad se otisak prsta skenira i analizira biometrijskim softverom. Jednom kad se odobri, biometrijski računalni sigurnosni sustav će unijeti informacije bankovnog računa korisnika, detalje kreditne kartice, te iznos plaćanja koji se želi potrošiti će biti skinut s računa. Korištenjem biometrijskog sustava, postoji vrlo mali rizik da se detalji s kreditne kartice ukradu, jamčeći dosta više sigurnosti za korisnika, [11].



Slika 2.8. Dijagram biometrijske naplate, [48].

3. Sustavi plaćanja elektroničkim novcem i sigurnosne značajke

Elektronički novac ili elektronička trgovina jedan je od načina ostvarivanja elektroničkog oblika plaćanja. Spomenuti oblik plaćanja pojavio se kao posljedica širenja Interneta i sve većih mogućnosti koje pružaju računalne mreže. U današnje doba vrlo je jednostavno obavljati kupovinu preko Interneta upotrebom kreditnih i bankovnih kartica, kao i elektroničkog novca. Stalno se povećava broj transakcija putem raznih vrsta bankomata, te pristup uslugama od kuće, telefonom ili osobnim računalom. Smanjuje se važnost poslovnica, a povećava se promet putem informatičkih mreža. Ovakvi trendovi povećavaju zadovoljstvo korisnika, a cijena transakcija se znatno smanjuje, [12].

Elektronički novac kao i gotovina mora imati svojeg nositelja. S obzirom na to, u praksi su se profilirala dva nositelja e – novca, na hardverski (opipljivi) i softverski. Hardverski je nastao ranije, a njegov nositelj je mikroračunalo u čipu na standardnoj platnoj kartici ili nekom drugom opipljivom mediju. Drugi je nastao pojavom Interneta, a nalazi se na serverima na mreži koji su imateljima dostupni preko mreže. Hardverski je nastao u Europi i u opticaju je u većini zemalja euro zone, a softverski je pristupniji u SAD – u odakle se širi globalno. Prvi je pogodan za neposredna plaćanja manjih iznosa i konkurentan je kovanicama i novčanicama manjih apoena, dok je drugi pogodan za elektronička plaćanja posredstvom Interneta i konkurentan je kreditnim karticama.

E – novac je uređen Zakonom o elektroničkom novcu i nekoliko podzakonskih akata. Za nadzor tog oblika plaćanja zaslužna je HNB[21] koja nadzire i regulira rad institucija za izdavanje elektroničkog novca. Institucije koje trenutno pružaju uslugu plaćanja e – novcem su telekomi i kartičarske kuće. Potencijal elektroničkog novca u bankarskom sektoru kod nas je još gotovo neiskorišten, djelomično i zbog manjkave infrastrukture, odnosno ne postoji ni jedan bankomat za punjenje elektroničkog novca, [12].

[21] **HNB** – Hrvatska Narodna Banka

3.1. Elektronički novčani sustavi

U tehničkom smislu, elektronički novac je virtualna reprezentacija, ili sustav debitnih i kreditnih kartica, koje se koriste za razmjenu vrijednosti s nekim drugim sustavom ili samim sobom kao zasebnim sustavom.

Elektronički novčani sustavi se mogu podijeliti na:

- notacijske sustave,
- simboličke sustave,
- centralizirane sustave,
- decentralizirane sustave, [12].

S obzirom na tip veze sustavi plaćanja e-novcem mogu se podijeliti u dvije skupine:

- *online* sustave – podrazumijeva postojanje stalne komunikacijske veze između osobe koja plaća i banke te se provjera valjanosti novčanice obavlja prije isporučivanja plaćene robe (npr. obavljanje kupovine kreditnim karticama),
- *offline* sustave – podrazumijeva povremenu vezu između osobe koja plaća i banke te se provjera valjanosti novčanica obavlja naknadno, nakon isporuke robe. Nakon obavljene transakcije serijski broj novčanice zapisuje se u bazu podataka banke, te se svaka daljnja novčanica s istim serijskim brojem dospjela na depozit odbija kao krivotvorina, [12].

3.1.1. Notacijski sustavi

Kod notacijskog sustava kupac koji ima otvoren račun u banci koristeći jedan od oblika bezgotovinskog plaćanja zapravo trgovcu predaje nalog za prebacivan je sa svog računa na račun trgovca. Radi se o elektroničkom nalogu, može biti e-ček, kreditna kartica, debitna kartica i slično, [13].

Kod ovih sustava transakcija je izravno ili neizravno vezana uz vrijednost pohranjenu negdje drugdje. Razlikuju se tri potkategorije notacijskih sustava:

1. narudžbe za elektroničko plaćanje prenošene preko mreže,
2. naplata kreditne kartice preko mreža,
3. notacijski sustavi temeljeni na pametnim karticama, [12], [13].



Slika 3.1. Presjek pametne kartice, [49].

Pametne kartice se mogu podijeliti prema tipu kontakta:

- kontaktne – podaci i/ili aplikacija pohranjena na čipu prenosi se preko elektroničkog modula koji je spojen na terminal ili čitač kartice,
- beskontaktne – ovakva kartica posjeduje antenu koja komunicira s antenom za primanje prilikom prijenosa podataka, [12].

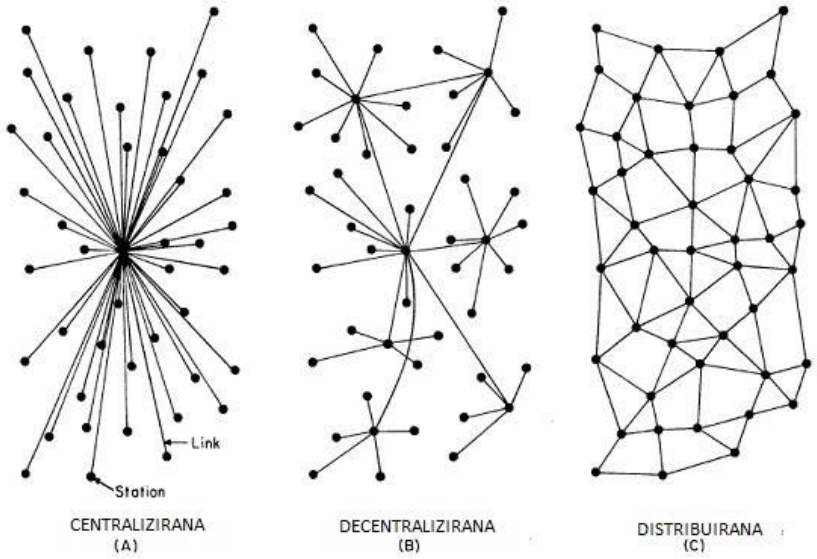
3.1.2. Simbolički sustavi

Za razliku od notacijskog sustava gdje novac zapravo nikada ne napušta banku, postoje sustavi kod kojih sama reprezentacija novca nosi njegovu vrijednost. To znači da se iznos na računu umanjuje čim se elektronička novčanica podigne iz banke. Ako se elektronička novčanica izgubi, vlasnik je bez nje ostao trajno. Ova vrsta elektroničkog novca analogna je klasičnoj gotovini i zato se obično naziva e-gotovina, [14].

3.1.3. Centralizirani sustavi

Centralizirani sustavi se temelje na „plaćanju unaprijed“ i mogu koristiti žetone, tj. objekte koji sadrže vrijednost. Korisnici moraju kupiti žetone od središnjeg autoriteta prije nego što mogu započeti transakciju. Postoje dvije potkategorije sustava sa žetonima:

- elektronički novac – zamjena papirnatog novca kao glavno sredstvo „online“ plaćanja,
- sustavi elektroničkog novčanika – temelje se na pametnim karticama koje koriste integrirane čipove za pohranu elektroničkog novca, [15].



Slika 3.2. Razlika između topologije sustava, [50].

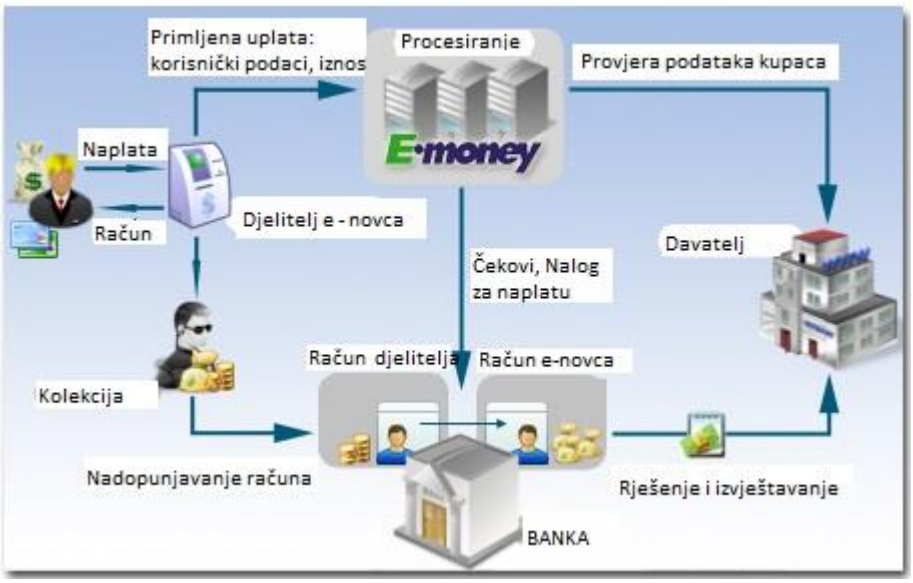
3.1.4. Decentralizirani sustavi

Jedan od najčešćih pristupa izgradnji raspodijeljene mreže je izgradnja partnerske mreže (engl. *peer-to-peer* – P2P). Rast popularnosti partnerskih računalnih mreža dogodilo se pojavom alata i servisa za slobodnu globalnu razmjenu datoteka. Raspodijeljeni sustavi sastoje se od međusobno povezanih čvorova koji se mogu samostalno organizirati u mrežne topologije sa svrhom dijeljenja raspoloživih resursa kao što su korisnički podaci, procesorsko vrijeme, kapacitet za pohranu podataka ili mrežna propusnost, te koji se mogu samostalno adaptirati na ispade funkcionalnosti i nepredvidive dolaske i odlaske čvorova na mreži, uz zadržavanje prihvatljive razine prospojenosti i performansi bez potrebe za nadzorom, kontrolom i podrškom iz jednog središnjeg mjesta, [12].

3.2. Primjena elektroničkog novca

Elektronički novac je stanje novca zabilježeno elektronički na kartici „pohranjene vrijednosti“. Te pametne kartice imaju ugrađen mikroprocesor koji može biti učitan s novčanom vrijednošću. Drugi oblik elektroničkog novca je mrežni novac, naročito Internet. Kao provjeravanje putnika, ravnoteža digitalnog novca je zahtjev privatne banke ili neke druge financijske institucije koja nije povezana na niti jedan određeni račun. Ovaj novac je izdan od javnih i privatnih institucija diljem svijeta i podizao je zabrinutost buduće sposobnosti središnjih banaka da postave ciljeve ponude novca. To se naširoko koristi u mjestima kao što su Njemačka, Nizozemska, Belgija, Singapur i Hong Kong, [16].

Samo definirani elektronički novac razlikuje se od takozvanih pristupnih proizvoda, koji omogućuju korisnicima da koriste elektronička sredstva komunikacije za pristup inače uobičajene platne usluge (npr. uporaba osobnog računala i računalne mreže za izvršenje plaćanja kreditne kartice). Bitna značajka ovih pristupnih programa je komunikacijska metoda (npr. uporaba računalne mreže prije nego da se posjeti banka), [16].



Slika 3.3. Princip rada elektroničkog novca, [51].

Razne sheme elektroničkog novca se razvijaju i znatno se razlikuju u svojim značajkama. Prvenstveno, produkti elektroničkog novca se razlikuju u njihovoj tehničkoj provedbi. Da bi pohranili vrijednost, sheme uključuju specijalizirane i prijenosne hardverske uređaje, tipični mikroprocesorski čip ugrađen u plastičnu karticu, dok softverski bazirane sheme koriste specijalizirani softver instaliran na standardnom osobnom računalu, [16].

Četiri vrste uslužnih davatelja su uključeni u rad sheme elektroničkog novca:

- izdavatelji vrijednosti za elektronički novac,
- mrežni operatori,
- prodavači specijalizirani za hardver i softver,
- omogućavatelji transakcija elektroničkog novca, [16].

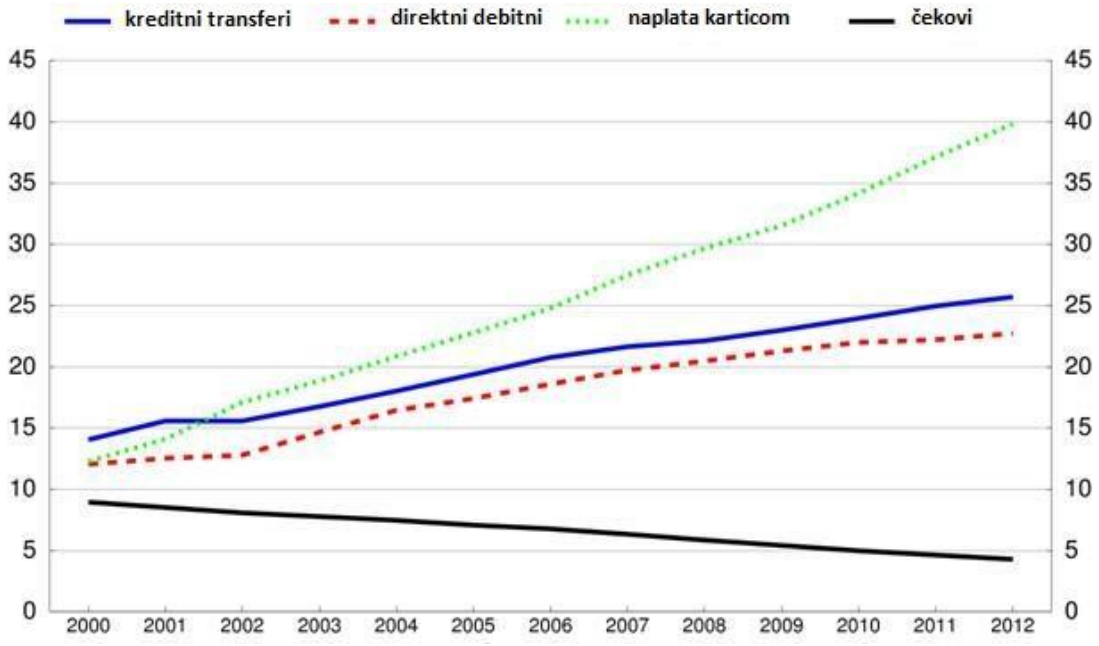
Neki sustavi elektroničkog novca omogućuju prijenose elektronskih stanja direktno od jednog potrošača prema drugom, bez prisustva treće osobe kao što su izdavatelji elektronskih vrijednosti. Većina sustava registrira određene pojedinosti u transakcijama između potrošača i trgovca u središnjoj bazi podataka. U slučajevima gdje su dopuštene direktne transakcije između korisnika, to se može jedino registrirati na korisnikovom vlastitom uređaju za pohranu, te može biti nadgledano centralno samo onda kad korisnik kontaktira davatelja usluga elektroničkog novca. U većini sustava elektroničkog novca trenutno se razvijaju i testiraju. Vrijednost pohranjena na uređaju je denominirana samo u nacionalnoj valuti, [16].

Elektronički novac je postao dio modernog bankarstva, te kao takav nastoji se usavršiti u vidu korištenja i sigurnosti. Neki od faktora koji utječu na razvoj imaju globalni karakter (nove informacijsko komunikacijske tehnologije, internet itd.), te sve ovise o stanju razvoja u jednoj državi. Faktori nacionalne razine su:

- razina razvoja države (utječe na kupovnu moć i ljudski životni standard),
- apsorpcijska moć za prihvaćanje tehnoloških inovacija,
- razvoj tržišta,
- regulatorni sustav,
- stupanj integracije u globalnoj ekonomiji i financijskom tržištu, [17].

Usporedba s ostalim instrumentima sustava naplate u Europskim državama daje jasnu sliku. Primjerice, transakcije sa debitnim/kreditnim karticama su oko 40 % od ukupnog broja platnih transakcija u usporedbi s transakcijama elektroničkog novca. Udio broja transakcija u elektroničkom novcu prema totalnom broju transakcija za sustav naplate u području Europe je bio samo 2,33% (2012.). Usporedba s prošlim godinama pokazuje blagi napredak (1.35% u 2008. godini i 1.70% u 2010. godini), [17].

Prema statističkim podatcima osiguranim od ECB[22] – a za određene Europske države, najveće godišnje povećanje transakcija elektroničkog novca je registrirano 2008. godine. Godišnja promjena je većinom tijekom transakcija u Luxemburgu, posebno za usluživanje transakcija elektroničkog novca. Jedna od najsnažnijih elektroničkih kompanija „Pay Pal" je preselio glavno sjedište sredinom 2007. iz Velike Britanije u Luxemburg, te u isto vrijeme su produžili dozvolu za elektronički novac. S novom dozvolom, pristup Pay Pal – u je bio moguć preko svih Internetskih stranica, u usporedbi s prošlošću kad je bio moguć samo preko stranica u Velikoj Britaniji, [17].



Slika 3.4. Statistika načina naplate do 2012. godine, [52].

3.3. Trendovi elektroničkog novca

Unatoč velikom interesu za elektronički novac koji se danas prikazuje, rijetko se može naići na informacije koje potvrđuju koju moguću poziciju elektronički novac može imati u

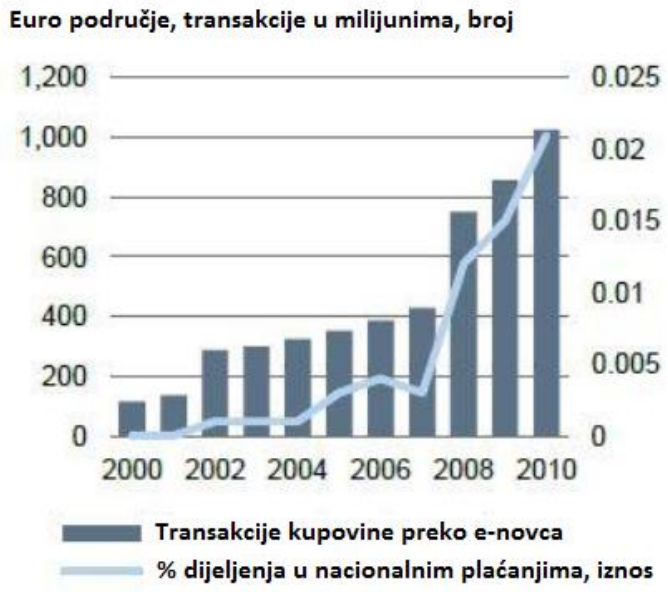
[22] **ECB** – Europska Centralna Banka

budućnosti, te kako korisnici vide cjelokupni proces korištenja elektroničkog novca. Upravo korisničko prihvaćanje je ključ za određivanje izvedivosti i učinkovitosti elektroničkog novca.

Danas postoje razna istraživanja korisničkog prihvaćanja uz anketiranje i definiranje rezultata. Rezultati istraživanja pokazuju koliko su korisnici zainteresirani za elektronički novac, te slične tehnološke inovacije. Glavni cilj istraživanja je proširiti znanje o trendovima elektroničkog novca i razumjeti faktore koji utječu na budući razvoj tržišta elektroničkog novca i prihvaćanje korištenja elektroničkog novca u različitim državama, [18].

Naročito glavni ciljevi su:

- Istražiti trenutni status korištenja elektroničkog novca za individualne i poslovne transakcije,
- Analizirati mišljenja ispitanika o elektroničkom novcu i prikazati osnovne prilike za buduće moguće promjene elektroničkog novca, [18].



Slika 3.5. Graf prikazuje porast kupovine s elektroničkim novcem, [53].

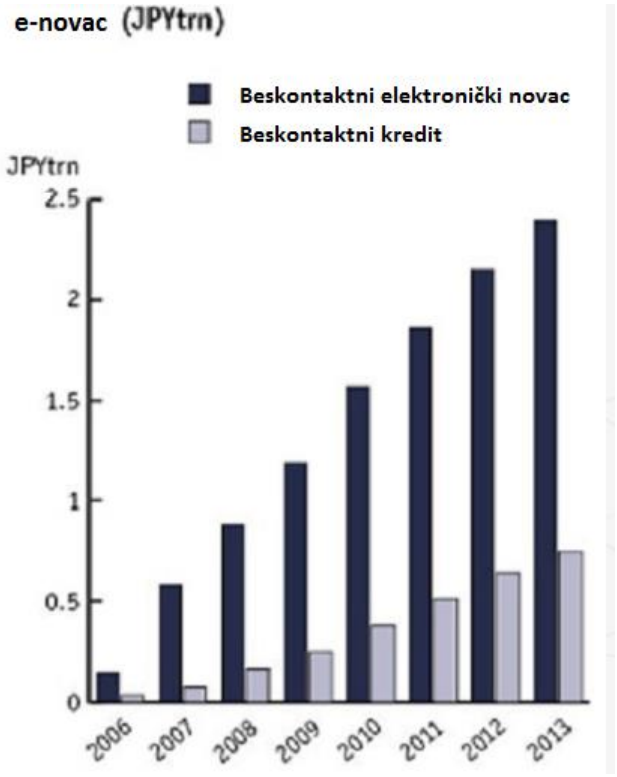
Relevantnost ove teme je vrlo visoka, zbog toga što je novac esencijalni atribut ekonomije tržišta. Stabilnost ekonomskog razvoja ovisi o protoku novca, te kako lako o brzo mogu biti novčane transakcije. U proteklih nekoliko godina se može zapaziti rapidna evolucija oblika novca, što vodi prema pojavi novih sredstava naplate. Svejedno, tržište

elektroničkog novca se upravo formira. Stoga, broj problema, posebno stvaranje tržišta elektroničkog novca, publika i sigurnost, regulatorna pitanja, te mnoga druga se trenutno slabije razumiju. Svrha ovakvih istraživanja je proučiti probleme i ključne trendove tržišta elektroničkog novca u Europi iz korisničke perspektive, [18].

Jedno istraživanje o korištenju elektroničkog novca provedeno u Finskoj 2013. godine je pokazalo da su mladi ljudi aktivni na Internetu, te koriste elektronički novac za razne aktivnosti. Došlo se do zaključka da su mladi motivirani za korištenje elektroničkog novca u budućnosti, unatoč nekim problemima. Ispitanici nisu imali konkretno mišljenje o pouzdanosti elektroničkog novca, što može biti dobar znak jer možda nisu imali / nemaju uopće sigurnosnih problema. Oni vjeruju da je moguće koristiti elektronički novac u svim aspektima života bez puno mentalnog napora. Međutim, još uvijek ne koriste elektronički novac više od gotovine ili bankovnih kartica, [18].

Može se primijetiti da elektronički novac danas nije toliko razvijen. Neki znanstvenici smatraju da će biti moguće da elektronički novac postane jedan od svjetskih valuta. Statistika ovog pojedinog istraživanja pokazuje da ljudi nemaju puno povjerenja u elektronički novac, te da elektronički novac neće nikad zamijeniti tradicionalnu gotovinsku naplatu. Iz odgovora možemo zaključiti da e – novac ima svoju poziciju u tržištu novca, ali se ne koristi uvijek u poslovne svrhe, nego će ga ljudi integrirati u svojim privatnim životima. Isto tako, bankomati, kreditne i debitne kartice su se masovno počeli koristiti tek nakon određenog vremena potrebnog da ljudi prihvate taj novitet.

Potrošači su stalno u potrazi za povećanjem brzine i jednostavnosti korištenja, te će s vremenom prijeći na račune elektroničkog novca, koje nude prednosti tradicionalnog bankovnog računa s dodatkom povećane privatnosti, smanjenja troškova, brže odgovore i poboljšanih korisničkih sučelja, [18].



Slika 3.6. Prikaz ubrzanog rasta trenda elektroničkog novca, [19].

Iz grafa iznad može se primijetiti da trend korištenja elektroničkog novca prilikom beskontaktne naplate se povećava sa svakom godinom. Vidljivi primjer postoji u Japanu koji prolazi kroz transformaciju u svojoj zaposlenosti alternativnih metoda naplate. U 2000., kad se elektronički novac pojavio imao je mali utjecaj na tržištu i regulatorima. Unatoč malim očekivanjima za ovu poziciju, elektroničko plaćanje se dramatično povećalo. Utjecaj beskontaktnih plaćanja na malim novčanim transakcijama, posebno u velikim gradovima ima tendenciju rasta. Svejedno, ukupna potrošnja je i dalje mala, unatoč velikim naporima da proširi svoju prisutnost, [19].

Prema jednom istraživanju tržišta elektroničkog novca provedenog u Japanu, postoji 98.4 milijuna uređaja u državi, uključujući pametne kartice i mobilne terminalne uređaje. Očekivan je stalan rast korištenja tijekom sljedećih pet godina. Beskontaktna plaćanja sastoje se od tri različite metode naplate: prepaid (pohranjena vrijednost), *auto – charge* (automatska nadopuna) i *post – pay*. Krajnje dvije su povezane s kreditnim karticama, što im pomaže ulasku u tržište plaćanja. Ključni čimbenici uspjeha uključuju povećanje broja trgovaca koji prihvaćaju beskontaktnu naplatu i promociju oba izdavatelja i distributera, [20].

3.4. Sigurnosni aspekti elektroničkog novca

Sigurnosne značajke u elektroničkim novčanim sustavima, kao i u drugim platnim sustavima su osmišljeni kako bi zaštitili integritet, autentičnost i povjerljivost kritičnih podataka i procesa, te zaštitili od gubljenja podataka, lažnih umnožavanja i odbacivanje transakcija, [20].

Sigurnosna mjerenja mogu biti podijeljena u nekoliko kategorija, te služe za detekciju, prevenciju i sadržaj prijetnji. Primarni cilj mjerenja služi za osiguranje da će napadi na bilo koju komponentu sustava biti spriječeni prije nego što se izvrši lažna transakcija. Mjere za otkrivanje mogu biti poduzete kako bi upozorili izdavatelja ili operatora sustava na pojavu prijevare i identifikaciju izvora prijevare. Mjere za suzbijanje su namijenjene za ograničenje opsega nakon počinjene prijevare. Određene mjere sigurnosti, osobito kriptografske tehnike su kritične za sigurnost elektroničkog novca tijekom faze sprječavanja, detekcije i očuvanja sigurnosti, [20].

Višestruka upotreba u transakcijama ili kopiranje istog elektroničkog novca sprječava se upisivanjem serijskog broja upotrebljavane novčanice u bazu podataka banke. Svaki put kad primi neku novčanicu, banka provjeri serijski broj u svojoj bazi podataka i zna da li je novčanica već bila upotrijebljena ili nije. Ako banka otkrije pokušaj prijevare, identificira osobu koja je pokušala prijevaru preko identificirajuće informacije, [21].

Po pitanju krivotvorenja e – novca, sigurnost je na najvišoj razini. Krivotvorenje elektroničkog novca nije moguće zbog toga što banka stavlja digitalni potpis na novčanicu i taj potpis nitko ne može falsificirati jer se obavlja tajnim ključem banke koji zna samo ona. Pri dolasku novčanice nazad u banku, ona provjerava svoj potpis i time se osigurava od novčanica koje je netko drugi generirao. Sigurnost sustava za elektroničko plaćanje ovisi o sigurnosti koju pružaju kriptografski algoritmi. Pod pretpostavkom da pri implementaciji kriptografskih algoritama i protokola nije učinjena nikakva greška, te da oni danas pružaju visok stupanj sigurnosti. Dalje ostaje mogućnost napretka kriptoanalize, te neizbježan ljudski faktor kojim se ta sigurnost može ugroziti, [21].

Sve vrste novca su mamac za varalice od davnih dana, elektronički novac nije iznimka. Istina je da se ne može lažirati na običan način, ali ipak prijevara u području elektroničke valute traži neku posebnu pozornost i posebne metode sigurnosti.

Koncept „lozinke“ je poznat svima, on uključuje ulaz niza karaktera poznatih samo određenom korisniku. U različitim sustavima naplate lozinka se može nazivati različitim imenima (kontrolni kod, PIN kod itd.), ali njezina suština je ista. Svaki kod se može koristiti samo jednom, nakon čega postaje nevažeći. Kontrolni kod se unosi prilikom izvršenja svake transakcije, te se koristi za dodatnu zaštitu, npr. da nositelj računa se prijavi na web stranicu računa, te se potom udalji s računala da ga ne ugasi. Lozinka, koja je poprilično jednostavan način za osiguranje sigurnosti e – novca je prisutna u različitim oblicima u svim sustavima elektroničke naplate. Nije najviše pouzdan način za osiguranje sigurnosti računa elektroničkog novca, te je to razlog zašto zaštita lozinkom je uvijek dopunjena drugim mjerama npr. kombinacija lozinke i potvrde kodova, [1].

Postoji još i zaštita ključnim datotekama koja je posebna datoteka za program elektroničkog novca, te sadrži podatke za autentifikaciju informacije. Ona služi za autentifikaciju korisnika prilikom pristupa računu Internet novca. Ova vrsta sigurnosti se primjenjuje osobito u „*WebMoney*“[23] naplatnom sustavu. Prilikom registracije, klijent prima datoteku koja sadrži ključeve. Bez ove datoteke, eventualni napadač, čak i ako zna lozinku, ne može otvoriti e – novčanik. Isto tako, samo ključna datoteka nije dovoljna za ulazak, nego je potrebno znati lozinku.

Uz razne jedinstvene mjere sigurnosti, postoji i tipkovnica na zaslonu. Umjesto utipkavanja verifikacijskog koda korištenjem tipkovnice računala, korisnik to može učiniti i s virtualnom tipkovnicom koja se prikazuje na ekranu, pritiskom na odgovarajuće brojeve s mišem. S jedne strane smanjuje sigurnost jer netko drugi može vidjeti verifikacijski kod, ali prednost mu je što štiti od „*keyloggers*“[24] napada. Još jedna vrsta zaštite je mogućnost blokiranja računa. Ova metoda zaštite elektroničkog novca se koristi ako ni jedna od dostupnih sigurnosnih mjera ne može više osigurati sigurnost sredstava na računu. U tom slučaju s pozivom, tekstualnom porukom ili online sustavom se zaključavaju korisnički računi, sprječavajući izvršenje bilo kakva transakcije, [1].

[23] **Webmoney** – globalni sustav rješenja i okruženja za online poslovne aktivnosti
[24] **Keyloggers** – vrsta nadzornog softvera koji ima sposobnost snimanja svakog pritiska na tipku koji se napravi u log datoteku.

3.3.1. Preventivne mjere

Elektronički uređaji koji se koriste za elektronički novac pružaju prvu liniju obrane od vanjskih napada. U sustavima baziranim na karticama, obrada povezana sigurnošću se izvodi u fizički osiguranom modulu, kao što je pametna kartica koja sadrži mikroprocesorski čip. Osiguran uređaj može biti pametna kartica ili kao što se često naziva SAM[25] – om, osigurana računalna komponenta integrirana u terminal za obradu plaćanja.

Annex 5 osigurava dodatne informacije o pametnim karticama i njihove sigurnosne značajke. Značajke otpornosti na prevaru ovih kartica su usmjerene na zaštitu podataka i softvera od neovlaštenih promatranja ili izmjena. Ove visoko softificirane značajke uključuju zajedno logičku (softversku) i fizičku (hardversku) zaštitu. Softverski kod se nalazi u čipu i osmišljen je kako bi zaštitio od bilo kojeg vanjskog promatranja ili izmjena. Zaštita softvera uključuje značajke aplikacije i operativnog sustava koji sprječavaju podatke pohranjene u memoriji od pristupa i mijenjanja osim za preferirane autorizacije i pristupne protokole. Često uključuje kriptografske tehnike, [23].



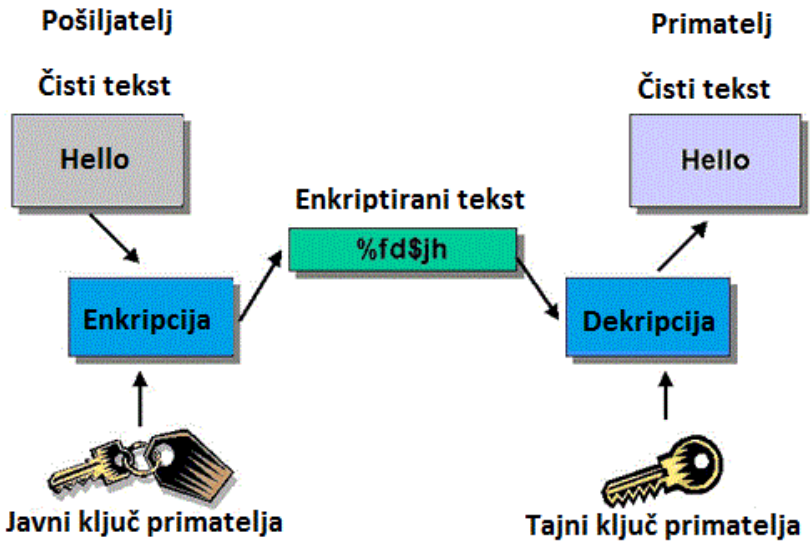
Slika 3.7. Izgled SAM kartice, [53].

Područja za pohranu podataka unutar pametne kartice sadrže različite razine sigurnosti. Svi podaci koji se ne mijenjaju tijekom života kartice se pohranjuju u memoriju samo za čitanje (ROM[26]). Osjetljivi, ali promjenjivi podaci se pohranjuju u EEPROM[27] dio memorije, koji se mogu mijenjati od strane internih funkcija čipa, [23].

[25] **SAM** – Sigurnosni Aplikacijski Modul
[26] **ROM** – Read Only Memory
[27] **EEPROM** – Elektronički izbrisivi programabilni ROM

Kriptografija je jedna od važnijih komponenti prevencije prevare u svim sustavima elektroničkog novca. Subjekt kriptografije je visoko kompleksan i pokriven je do zadnjeg detalja u Annexu 7. Kriptografske tehnike omogućavaju logičku zaštitu sustava elektroničkog novca osiguravajući povjerljivost, autentičnost i integritet uređaja, podataka i komunikacija korištenim u transakcijama.

Enkripcija je tehnika korištena za zaštitu povjerljivosti podataka tijekom transmisije ili dok je spremljena na uređaju. Enkripcija je osobito najvažnija za određeni dio osjetljivih podataka korištenim u sigurnosnim postupcima, kao što su kriptografski ključevi. Ostale informacije, kao što su plaćanje iznosa i serijski brojevi kartica, ne moraju nužno biti preneseni ili spremljeni u enkripcijski oblik. Kriptografija se također koristi u nekim sustavima za potvrđivanje valjanosti elektroničkih bilješka ili druge podatke stvorene od strane izdavatelja ili operatora sustava. Sigurnost sustava barem djelomično ovisi o kriptografskoj zaštiti elektroničkih bilješki što je obično ovjereno s digitalnim potpisom. Taj pristup je čest u sustavima baziranim na softveru, u kojem se iznosi ne mogu zaštititi fizički, već matematički, [23].



Slika 3.8. Primjer enkripcije, [54].

Digitalni potpis kao dio kriptografije predstavlja metodu za potpisivanje poruka u elektronskoj formi. Tako potpisana poruka može se prenositi računarskim mrežama. Ipak, treba biti oprezan jer kopija digitalno potpisane poruke identična je originalu, za razliku od poruke koja je na papiru potpisana na konvencionalan način. Digitalni potpis predstavlja kriptografsko obilježje poruke potpisnikovim tajnim parametrom. Digitalni potpis je kriptosustav s javnim ključem koji omogućuje prenošenje korisnih svojstava konvencionalnog papirnog potpisa u digitalni svijet, [24].

Međutim, ono što je vrlo bitno, digitalni potpis omogućuje:

- autentifikaciju – osoba B može provjeriti je li poruka koju je primila zaista poslala osoba A,
- nepobitnost – osoba A ne može poreći da je ona poslala poruku ako osoba B posjeduje poruku s njenim potpisom.

Na ovaj način, u slučaju spora obje strane u potpunosti su zaštićene digitalnim potpisom.

Za zaštitu se koristi i digitalni slijepi potpis, s kojim se potpisuju elektronički elementi gdje se sudionik autentificira tako da nije odan njegov identitet (npr. anonimnost u glasovanju). Budući da slijepi potpis pruža potpunu nepovezanost, nemoguće je povezati par poruka, ali ipak ta anonimnost se može zloupotrijebiti od strane kriminalaca. Zbog toga, bilo bi korisno kad bi se anonimnost mogla ukloniti uz pomoć pouzdanog identiteta, kada je potrebno zbog pravnih razloga. Zato je predložena nova vrsta slijepog potpisa, pošteni slijepi potpis. Takva vrsta potpisa ima svojstvo da je moguće povezati par poruka (potpis) uz odgovarajući pregled protokola potpisivača, [25].

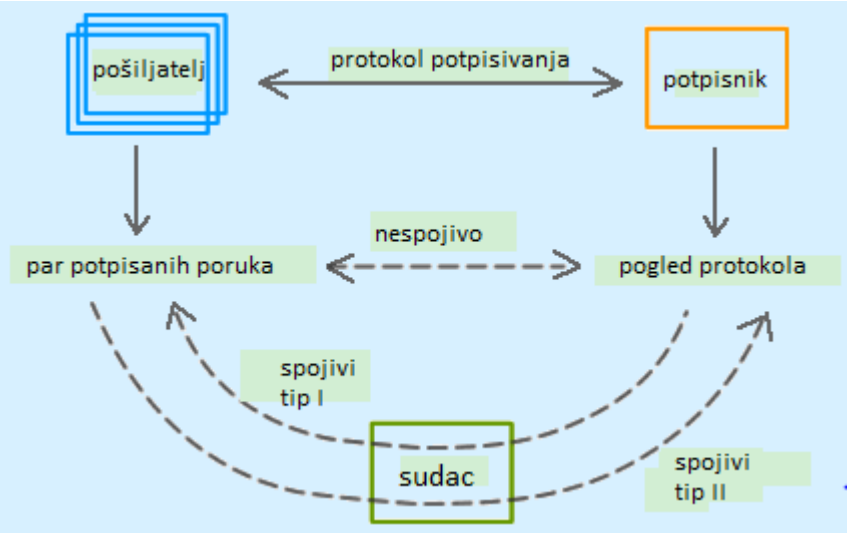
Model sustava poštenog slijepog potpisa sastoji se od nekoliko pošiljatelja, jednog potpisivača, jednog suca i dva protokola:

- protokola potpisivanja koji uključuje potpisivača i pošiljatelja,
- protokola obnavljanja veze koji uključuje potpisivača i suca.

Obavljanjem protokola potpisivanja, pošiljatelj dobiva valjan potpis poruke po njegovom izboru, takav da potpisivač ne može povezati svoje gledište protokola s rezultirajućim parom poruka (potpis). Izvođenjem protokola za obnavljanje veze, potpisivač od suca dobiva informaciju koja mu omogućava da prepozna odgovarajući pogled protokola i par potpisanih poruka. Pošteni slijepi potpis ima različitih primjena, jedna je pružanje alata za sprječavanje pranja novca u sustavima plaćanja s anonimnošću, [25].

Namjena mu je u aplikacijama vezanim za elektronički novac. U svakom trenutku digitalni slijepi potpis mora zaštititi identitet korisnika. Elektronički novac je zbog toga nemoguće pratiti jer ne ostavlja traga zbog slijepog digitalnog potpisa, a moguće su prijevare i pranje novca.

Pravedni digitalni potpis sastoji se od dva protokola između korisnika (*sender*), banke (*signer*) i treće strane – suca (*judge*). Prvi protokol „*signing*“ se koristi u komunikaciji korisnika i banke (slijepi potpis), [25].



Slika 3.9. Princip komunikacije prilikom izrade potpisa, [25].

Drugi protokol „*link recovery protocol*“ koriste banka i sudac. Banka dobiva informaciju potvrde i pregled protokola, dok sudac može implementirati dva tipa pravednog slijepog potpisa ovisno o dobivenim informacijama. Opisani protokoli narušavaju anonimnost slijepog digitalnog potpisa i omogućuju policiji da uslijed kriminalne radnje dođe do informacija o pošiljatelju. U drugoj izvedbi pravednog slijepog potpisa korisnik povjerava svoje informacije trećoj povjerljivoj strani koja vrši provjeru potpisa za nekoga. Slijepi digitalni potpisi se najčešće implementiraju u sustave koji omogućuju elektroničku naplatu, te da osiguraju sigurne transakcije i nemogućnost povezivanja korisnika s transakcijom.

Osim gore navedenih sustava digitalnih potpisa postoji još mnogo sustava digitalnog potpisa koji pružaju dodatnu funkcionalnost. Jednostruki digitalni potpis je mehanizam za potpisivanje koji se može koristiti za potpisivanje najviše jedne poruke inače bi se potpisi mogli krivotvoriti. Jednostruki potpisi su pogodni za primjenu u pametnim karticama, gdje je potrebna mala računska složenost, [25].

3.3.2. Mjere detekcije

Pojedine transakcije elektroničkog novca, jedanput izvršene su predmet postupaka nadzora i provjere sigurnosti. U većini sustava baziranim na karticama koje su analizirane, pojedina transakcija se može prepoznati po jedinstvenom broju, baziranom na serijskom broju kartice i njegovog brojača transakcije, koji se povećava za jedan broj za svaki pokušaj transakcije.

Transakcije mogu biti predmet financijske provjere, kao i sigurnosne provjere. Financijska provjera može uključivati nagomilane transakcijske iznose za svaki uređaj i izračun stanja pojedinog uređaja, koji su pohranjeni u centralnoj bazi podataka. Iako se točno stanje računa pojedinog uređaja u bilo kojem trenutku ne može izračunati s potpunom točnošću zbog vremenskih stanki u transakcijama. Ova vrsta aktivnog praćenja transakcija pruža visok stupanj sigurnosti da bilo koja lažna transakcija ili promjena stanja računa na kartici će biti otkrivena u jednom trenutku. Vrijeme koje može proteći prije detekcije bi se moglo znatno razlikovati ovisno o dizajnu određenog sustava. Neki sustavi elektroničkog novca ne provjeravaju svaku transakciju protiv centralnog održanog stanja, zato što se ne prikupljaju rutinski svi podaci transakcije ili iz troškovnih razloga, [23].

Online interakcija s izdavateljem ili središnjim upraviteljem sustava elektroničkog novca je obično korištena sigurnosna značajka sustava baziranom na karticama. Takva interakcija dopušta središnjem operatoru da provjeri sigurnosne parametre kartice za konzistentnost, za ažuriranje sigurnosne mjere na uređaju, kao što su kriptografski ključevi. Transakcijska registracija i snimak bilo kakve pogreške ili nepotpune transakcije može biti pročitana i pohranjena u središnjem sustavu. Takve mjere povećavaju vjerojatnost da će bilo koji pokušaj prijevare biti otkriven u kratkom razdoblju. Događaji koji mogu zahtijevati interakciju sa središnjim sustavom uključuju rutinsko punjenje i depozitne transakcije, rješavanje neuspješnih transakcija ili višestrukih neuspjelih pokušaja za unos PIN[28] – a. Online transakcijom se može također pokrenuti datum isteka uređaja ili stanje računa. U nekim sustavima, ili nekim planiranim poboljšanjima, uređaj će sam automatski prestati raditi nakon određenog broja uzastopnih „*offline*“ transakcija, jer su zahtijevale mrežne interakcije. Neke od tih mjera mogu smanjiti praktičnost i fleksibilnost za nositelja kartice, [23].

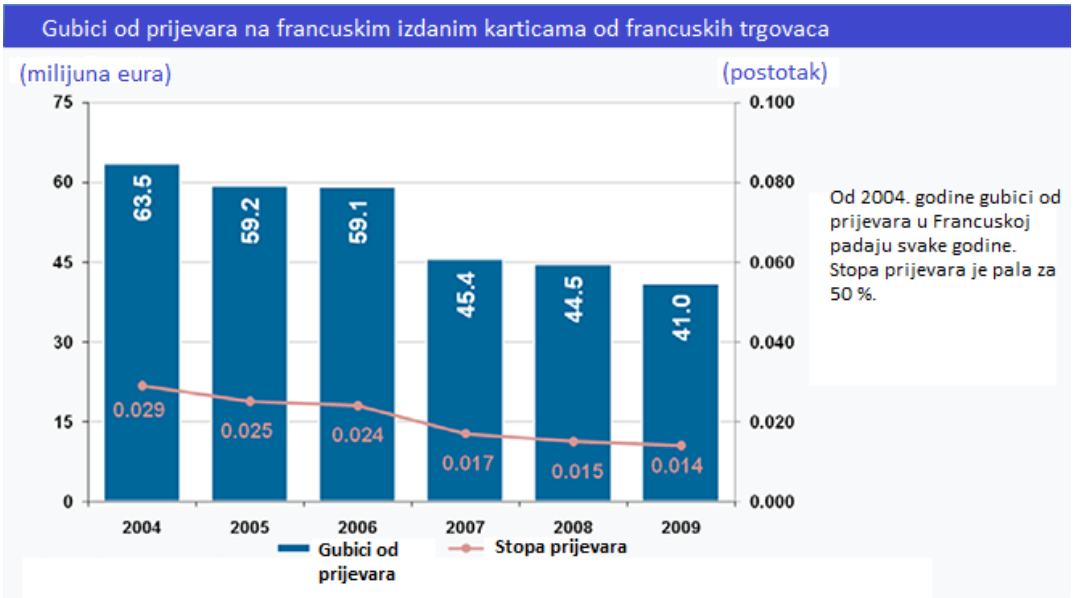
[28] **PIN** – Personal Indentification Number

3.3.3. Mjere za suzbijanje

Dopuštena ograničenja na veličinu stanja na kartici koje su pohranjena na potrošačkom i trgovačkom uređaju su vrlo važna sigurnosna značajka sustava elektroničkog novca. Sustavi bazirani na bilješkama ne smiju sadržavati izravno ograničenje iznosa, ali u nekim slučajevima mogu ograničiti broj denominacije bilješki izdanih s određene kartice u bilo kojem trenutku. Dok izravni učinak granica vrijednosti služi da sadrži veličinu gubitaka od uspješnih pokušaja prijevare, neizravni preventivni rezultat može biti jednako važan – kako bi zadržao pokušaj prijevare smanjujući potencijalnu financijsku dobit.

Svaki napadač će morati udvostručiti ili mijenjati velik broj kartica kako bi se trud isplatio financijski. Ograničenje stanja računa oslanja se vrlo siguran način za pohranjivanje maksimalne granice ravnoteže kako bi se spriječila oštećenja. Ograničenja na potrošačkim karticama ne smiju pomoći sadržavati načine za kršenje sigurnosti.

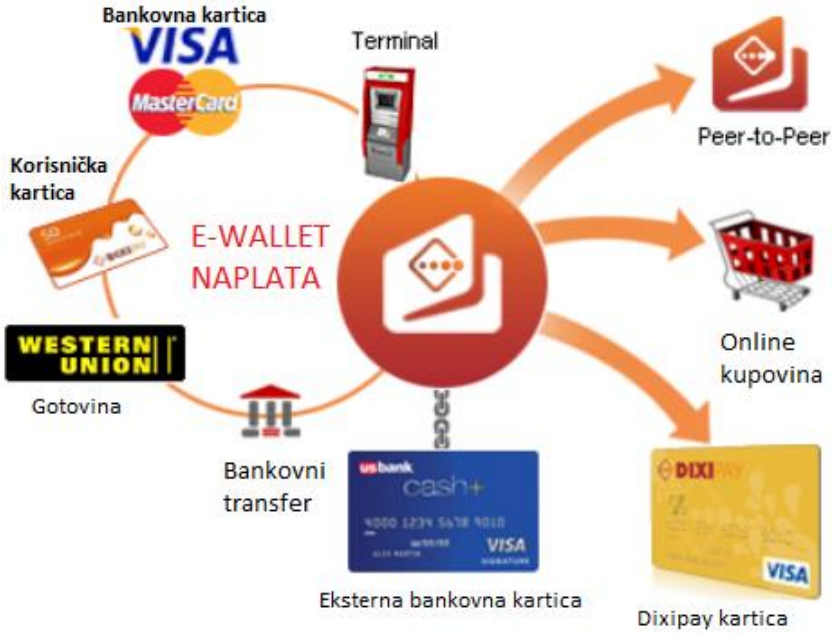
Datumi isteka na karticama i na računu također služe da sadrže obujam bilo koje prijevare, tako kartica promijenjena prijevarom će biti korisna samo na određeno vrijeme. Važno je da se takve mjere mogu koristiti za prisilu korisnika na interakciju sa središnjim sustavom, gdje prijevara može biti lakše otkrivena. U sustavima baziranim na karticama, kartice mogu sadržavati ograničenja na maksimalni broj transakcija koje određena kartica može obavljati, [23].



Slika 3.10. Grafikon koji prikazuje gubitke sa prijevarom na karticama u Francuskoj, [55].

4. Značajke i arhitektura platforme Google Wallet

Digitalni novčanik odnosi se na elektronički uređaj koji omogućuje pojedincu da obavi transakcije elektroničke trgovine. To može uključivati kupnju proizvoda online na računalu ili korištenjem pametnih terminalnih uređaja za kupovinu. S vremenom, digitalni novčanici su napravljeni ne samo za osnovne financijske transakcije, nego i za autentifikaciju korisnika koji posjeduje e – novčanik. Primjerice, digitalni novčanik može potencijalno provjeriti dob kupca prilikom kupovine alkohola u trgovini. To je korisno za pristup pojmu „digitalnog novčanika“, ne kao jedinstvenoj tehnologiji, već kao tri glavna dijela: sustav (elektronička infrastruktura), aplikacija (softver koji radi na vrhu) i uređaj (individualni dio), [26].



Slika 4.1. Prikaz sustava elektroničkog novčanika, [56].

Na slici iznad prikazan je sustav elektroničkog novčanika te sve komponente s kojima e – novčanik ima interakciju. Vidljivo je da elektronički novčanik ima više načina sredstava naplate, te je povezan s bankom. Omogućuje obradu financijskih transakcija prilikom kupnje određenog proizvoda „*online*“, slanje novčanih iznosa drugom e – novčaniku ili računu, te pohranu novčanih iznosa na „Dixipay“[29] karticu.

[29] **Dixipay** – su u potpunosti osigurane online financijske usluge plaćanja za pojedince ili poduzeća, omogućuju instantno slanje i primanje novca preko Interneta, računa trgovca i usluga naplate elektroničke trgovine.

Google Wallet je sustav mobilne naplate razvijen od Google – a koji omogućuje svojim korisnicima pohraniti debitne kartice, kreditne kartice i poklon kartice, te mnogo ostalih mogućnosti. Google Wallet koristi NFC[30] tehnologiju, pomoću koje izvršava naplatu prislanjajući pametni telefon na naplatni terminal. Koristeći NFC i Cloud tehnologiju, Google Wallet omogućuje ljudima da izvršavaju brze i sigurne naplate. Korisnici mogu na mreži (web stranicama) koristiti svoj Google Wallet račun gdje je prisutno „*Google Wallet Buy*“ dugme.

Osim za pohranjivanje podataka o kreditnoj kartici, Google Wallet sadrži i kartice za odanost i poklon kartice na svojim mobilnim uređajima i iskorištavanje prodajnih promocija koristeći aplikaciju. Sve kreditne i debitne kartice su pohranjene na sigurnim Googleovim poslužiteljima sa sljedećim komponentama sigurnosti:

- Mogućnosti zaključavanja: Na pametnom mobilnom uređaju, 4 – znamenkasti Google Wallet – ov osobni identifikacijski broj (PIN) sprječava neovlašteni pristup informacijama o kreditnoj kartici. Google ima na mreži više slojeva zaštite s lozinkom da bi pomogao stvaranju obrane od „*cyber*“ kriminalaca ili kreditnih prijevara.
- Daljinsko upravljanje: Google Wallet računi mogu biti onesposobljeni s udaljenosti u slučaju gubitka pametnog mobilnog uređaja. Pojedinačne kartice će i dalje raditi, ali Google Wallet kupnje preko mobilnog terminalnog uređaja će biti onemogućene.
- Enkripcija: Kreditne i debitne kartice pohranjene u Google Wallet – u su kriptirane na Google – ovim sigurnim serverima na sigurnoj lokaciji. Kada korisnici plaćaju u trgovini, Google plaća trgovca, a zatim obrađuje transakciju s korisnikovom odabranom kreditnom i debitnom karticom. Ova informacija jamstva plaćanja karticom je od trgovca, te Android operacijskog sustava.
- Skriveni brojevi računa: Aplikacija čuva brojeve računa naplatne kartice skrivenima. Kada se kartice pojave na ekranu korisnikovog mobilnog uređaja u trgovini, brojevi nisu vidljivi. Na mreži su vidljive samo 4 zadnje znamenke tijekom kupnje, [26].

[30] **NFC** – Near Field Communication

Google Wallet verzija 1.0 je lansirana 2011. godine. Ta početna verzija softvera je mogla pokrenuti samo na Google Nexus S mobilnom terminalnom uređaju, koji je bio jedan od prvim mobilnih uređaja s ugrađenim NFC čipom. Google je udružen s MasterCardom, kreirajući put za Google Wallet 1.0 da bi predstavio MasterCard od Citibank – a[31], ali Google je očekivao tehnologiju za rad sa svim velikim kreditnim karticama u budućnosti. Google Wallet prihvaća 150 000 trgovaca u SAD – u i 230 000 u inozemstvu. Zapravo, Europljani i Azijati rutinski koriste tehnologiju pametnih mobilnih uređaja za obradu plaćanja, [27].

Korisnik Google Wallet – a mora namjestiti četveroznamenkasti PIN broj, koji se unosi prije kupnje. Iako to smanjuje praktičnost SingleTap - a[32], Google čvrsto vjeruje da je PIN osnovna sigurnosna mjera koja sprječava neovlaštene kupnje u slučaju gubitka ili krađe mobilnog uređaja.



Slika 4.2. SingleTap NFC tehnologija, [57].

Google Wallet pohranjuje informacije korisničke kreditne kartice u šifriranom obliku na računalnom čipu pametnog telefona koji je poznat kao „Secure Element“. Taj čip je odvojen od memorije telefona i dostupan je samo preko programa sigurnosnog elementa. Ovaj sustav štiti informacije korisničke kreditne kartice i prenosi se iz mobilnog uređaja na NFC čitač. Da bi se spriječila prijevara provlačenja kartice, NFC čip je kompletno deaktiviran dok je ekran mobilnog uređaja isključen, [27].

[31] **Citibank** – potrošačka podjela financijskih usluga multinacionalnog Citigroup – a (Američke multinacionalne banke)
[32] **SingleTap tehnologija** – tehnologija naplate koja se koristi s NFC terminalom, te izvršava naplatu prilikom približavanja mobilnog uređaja terminalu.

4.1. Zaštita od prijevare

Google Wallet zaštita od prijevare pokriva 100% svih ovjerenih neovlaštenih transakcija u Sjedinjenim Američkim Državama. Da bi korisnik mogao biti pokriven s tom policom, mora biti stanovnik SAD – a i imati američku adresu povezanu s računom Google Wallet-a. Osim toga, neovlaštene aktivnosti moraju se prijaviti u roku od 120 dana od dana transakcije. Sve transakcije se prate od 0-24 sata za prevarljive i neovlaštene aktivnosti od strane tima za sigurnost, a tim za podršku je na raspolaganju pomoći s bilo kakvim pitanjima o Google Wallet usluzi.

Tijekom korištenja aplikacije sve financijske informacije su zaštićene i kriptirane, te Google Wallet zaštita kupnje pokriva sve opravdane neovlaštene transakcije. Dok je ova Google-ova značajka popularna i korisna, iskorištena je od raznih prevaranata koji se nadaju ukrasti novac od nesumnjivih korisnika stvaranjem lažnih računa koji izgledaju slično kao originalni Google Wallet račun, [28].

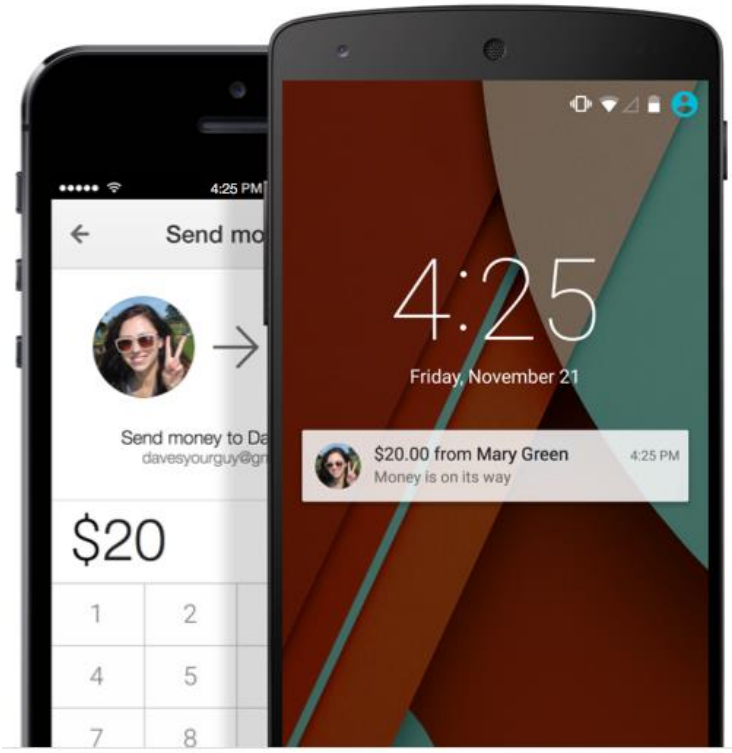
Neki od znakova opasnosti iza kojih stoje prevaranti:

- Ako Google provjera plaćanja podržava samo kreditne ili debitne kartice. Te ako prodavač sugerira žično (*online*) plaćanje (Western Union, MoneyGram) ili prijenos novaca s banke, vjerojatno se radi o prijevari.
- Prevaranti mogu obavještavati o određenim pojmovima kao što su: „Potvrđeni Googleov agent za provjeru plaćanja“, „Regionalni menadžer“, „Račun za zaštitu prilikom kupnje“ ili neki drugi oblik „*escrow* računa[33]“ u njihovom lažnom računu.
- Prevaranti mogu tražiti velike iznose transakcije novca kako bi ih podijelili u manja plaćanja.
- Cijena proizvoda za koju su kupci zainteresirani izgleda „predobra da bi bila stvarna“ ili prodavatelj tvrdi da ima novi dobar proizvod koji se svugdje odlično prodaje, [29].

[33] **Escrow račun** – je račun na koji jedna ugovorna strana u nekom trgovačkom ugovoru preda escrow - novac, vrijenosnice ili dokumente banci u polog na čuvanje, s tim da je banka ovlaštena položeni novac isplatiti ili dokumente izručiti njegovoj drugoj ugovornoj strani (korisniku), pod uvjetima koji su utvrđeni ugovorom između banke – escrow agenta, nalogodavca i korisnika.

4.2. Sigurnosni aspekti

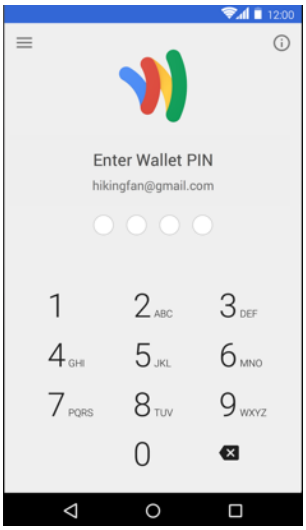
U slučaju da se mobilni terminalni uređaj izgubi, može se preko računa na Internetu onemogućiti Google Wallet aplikaciju. Ako se izgubi Wallet kartica, korisnicima se nudi mogućnost privremenog zaključavanja preko aplikacije. Ako korisnik primijeti bilo kakve sumnjive aktivnosti trošenja na svom računu, može ih pronaći na listi transakcija i podnijeti zahtjev u kojem prijavljuje neovlaštene naplate. Aplikacija šalje instantne obavijesti korisniku prilikom svakog slanja i primanja novca, te obrađene transakcije Google Wallet karticom. Postoji mogućnost praćenja transakcija u aplikaciji i na *web* stranici, [30].



Slika 4.3. Mogućnost praćenja transakcija, [30].

Google Wallet iz dana u dan razvija sve više sigurnosnih elemenata, dok s druge strane uspješno eliminira pokušaje prijevare. Korisnici su dosta skeptični prema sigurnosti ove usluge, ali Google radi na tom području, te je jasno da će takvih sigurnosnih propusta biti sve manje. Sigurnost je jako bitna stavka ove usluge, te je očigledno da se ne smije zanemarivati. Iako je izumljen još 2011., Google Wallet i dalje ima status poprilično nesigurne usluge, a najavljena je uskoro poboljšana verzija u kojoj bi trebali sigurnosni propusti biti riješeni.

Da bi se korisnici zaštitili od neovlaštenog korištenja Google je osmislio zaključavanje aplikacije PIN brojevima, te zaštitu enkripcijom. Pristup omogućuje ispravno unesen 4 – znamenkasti osobni identifikacijski broj. PIN se upotrebljava za otključavanje, slanje novca ili podizanje novca s bankomata pomoću Google Wallet kartice, [30].

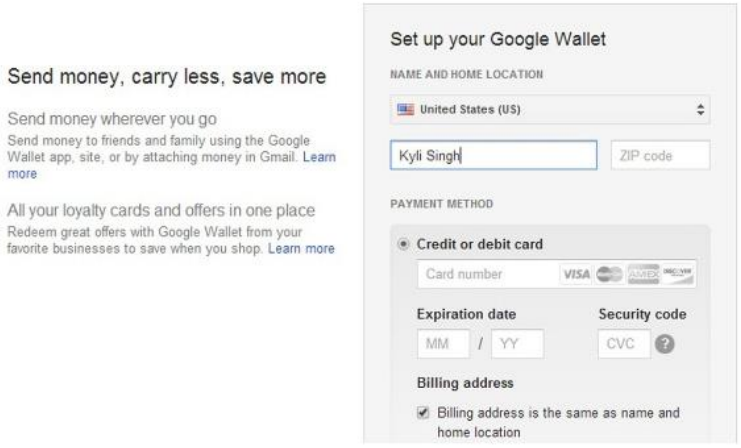


Slika 4.4. Korištenje PIN – a, [30].

Google Wallet radi samo s uređajima koji podržavaju sigurnosni čip (*Secure Element chip*). Sigurnosni čip je dizajniran za pohranu informacija o naplati odvojeno od operacijskog sustava i glavnog hardvera. Svi podaci naplate koji su pohranjeni u čipu na mobilnom terminalnom uređaju su kriptirani. To znači da se podaci mijenjaju (kodiraju) prije nego što se šalju, dok kad dostigne odredište dekodiraju se koristeći algoritam za dešifriranje informacija. Enkripcija je posebno važna kad se koristi NFC tehnologija na uređaju osiguravajući da prava osoba izvršava transakcije, te osigurava da podaci ne mogu biti pročitani čak ni tijekom transakcije. Pomoću NFC tehnologije korisnik može izvršiti naplatu bežično preko mobilnog uređaja i naplatnog terminala. NFC je dizajniran da radi samo kad je upaljen ekran korisnikovog mobilnog uređaja, te dok je udaljenost između uređaja i terminala do nekoliko centimetara, [31].

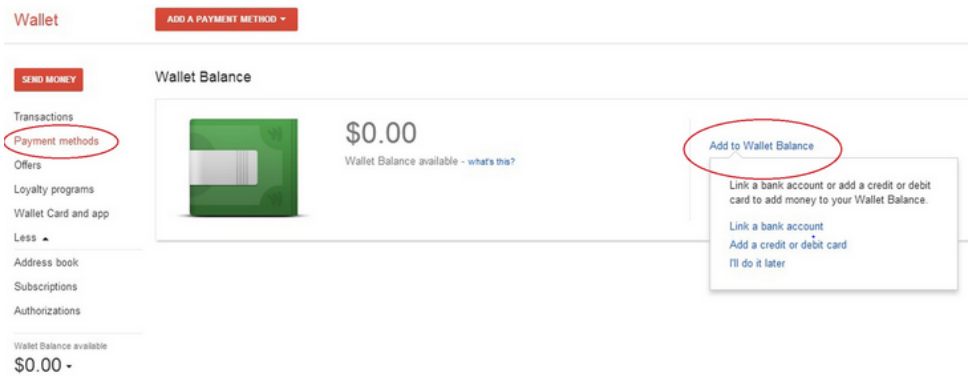
4.3 Osnovno korištenje aplikacije

Za početak korištenja Google Wallet aplikacije zahtjeva se izrada Google računa na mreži ukoliko korisnik isto nema. Prilikom izrade računa, odnosno prijave na račun zahtjeva se upisivanje osnovnih podataka i podataka o kreditnoj kartici, [32].



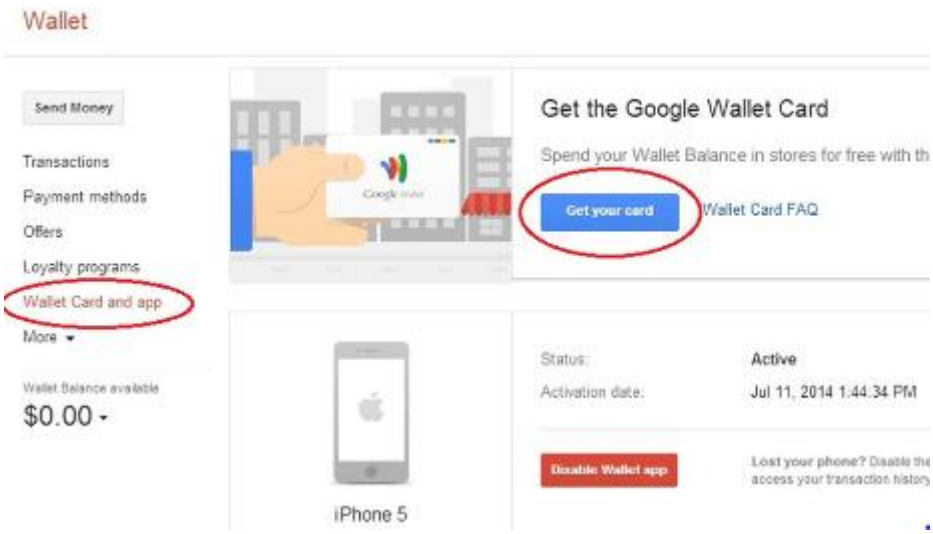
Slika 4.5. Prikaz prozora za popunjavanje podataka, [32].

Nakon prijave, Google traži provjeru identiteta korisnika, te aktivaciju Google Wallet kartice sa sigurnim praćenjem protiv prijevara. Kad se provjeri identitet, korisnik mora kreirati 4 – znamenkasti PIN koji će mu osiguravati dosljednu provjeru sigurnosti i zaštitu od neovlaštenog korištenja. Nakon izrade računa, kreiranja PIN – a, te instalacije aplikacije na mobilnom uređaju korisnik može napuniti svoj račun s određenom svotom novca. Stanja novca u aplikaciji je novac pohranjen u virtualnom novčaniku. S tim stanjem računa, korisnik može slati novac na druge račune, kupovati na Internetu i kupovati u trgovini pomoću uređaja (NFC). Korisnici imaju mogućnost i dodavati novac direktno preko banke potpuno besplatno, dok se za preuzimanje novca s kreditnih ili debitnih kartica uzima provizija od 2.9 %, [32].



Slika 4.6. Prikaz načina dodavanja novca na račun, [32].

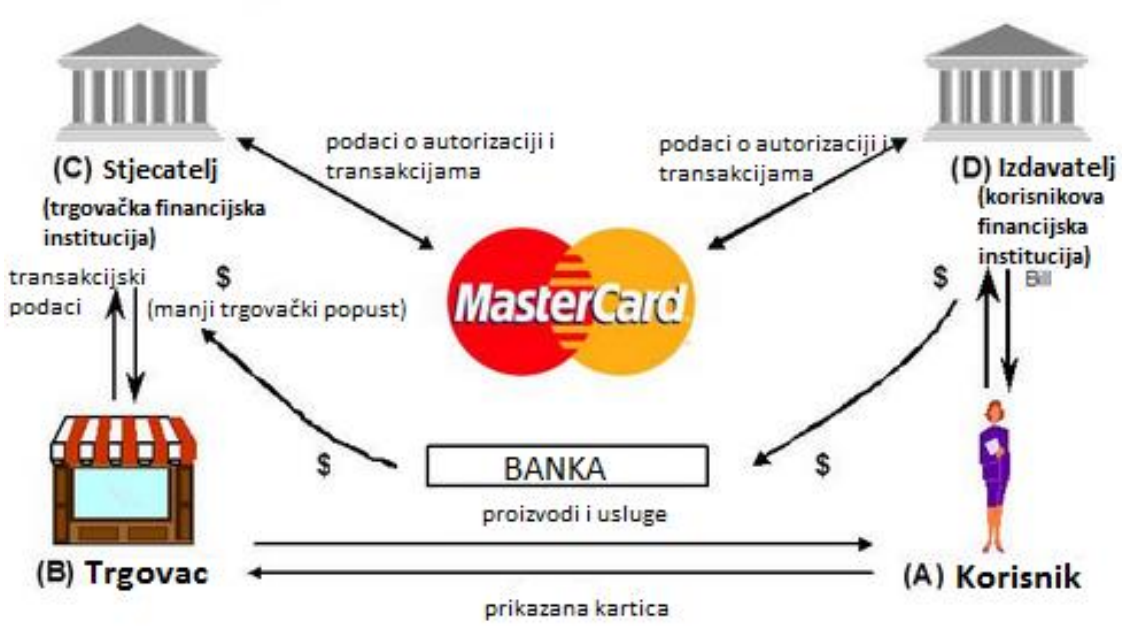
Da bi korisnik koristio Google Wallet kupovnu karticu istu mora i aktivirati. Kartica je povezana s računom i može se koristiti za kupnju unutar trgovine. Na *web* stranici korisnik odabire „*Wallet card and app*“ dugme, te nakon provjere identiteta nabavlja i naručuje karticu. Nakon aktivacije kartice bude automatski poslana na kućnu adresu korisnika, [32].



Slika 4.7. Način aktiviranja i nabavke kupovne kartice, [32].

Za korištenje u trgovinama korisnik treba odabrati kreditnu ili debitnu karticu s koje će mu biti povučen novac. Kartice je prihvatljiva u mnogo „MasterCard“ lokacija i korisnik ima mogućnost potrošiti 5000 $ (dolara) svakih 24 sata. Limit ne uključuje podizanje novca s banke ili bankomata. Ako se koristi mobilna aplikacija na Android mobilnom uređaju, korisnik može jednostavno približiti mobilni uređaj terminalu za naplatu uz pomoć NFC tehnologije, te tako izvršiti naplatu. Mobilni uređaj se mora držati 5 cm od naplatnog terminala, te potom korisnik upiše svoj PIN i naplata se jednostavno izvrši, [32].

Za slanje novca drugim osobama (računima), korisnik može koristiti dugme „*Send money*“ na desktop ili mobilnoj aplikaciji. Ako korisnik nije uspješno potvrdio svoje informacije ili preskočio taj korak, aplikacija će ga upozoriti da potvrdi još jednom. Informacije se mogu potvrditi preko mobilnog uređaja ili preko popunjavanja online formulara. Jednom kad se potvrdi identitet, korisnik ima mogućnost brzo i lako slati novac u SAD – u preko *e-mail* adrese, [32].

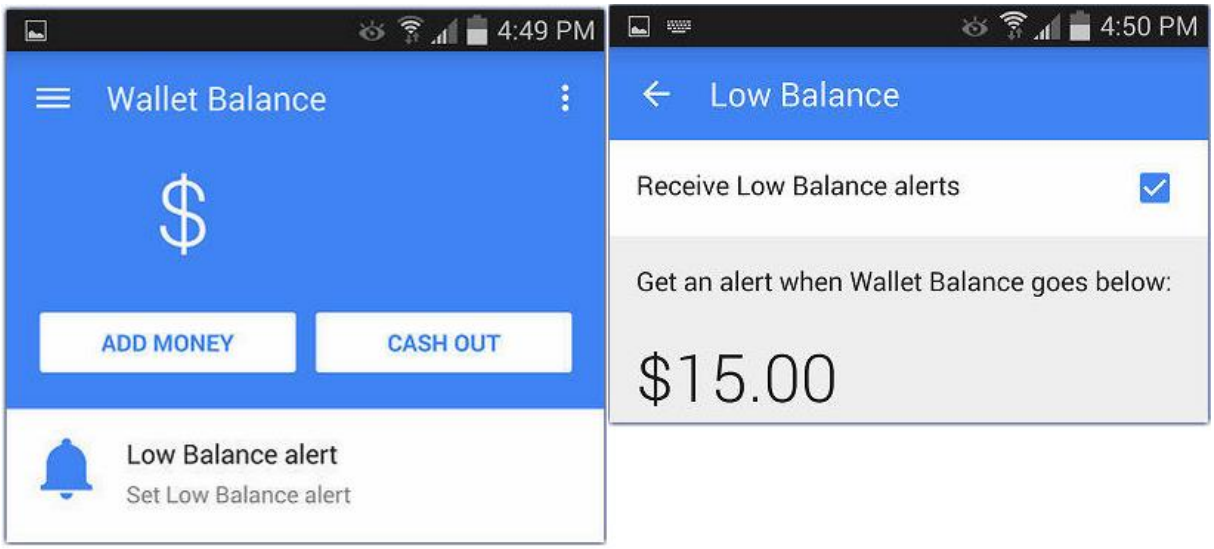


Slika 4.8. Interakcija kartične transakcije, [33].

Prilikom tipične transakcije korisnik kartice (A) kupuje proizvode od trgovca (B) korištenjem uređaja za naplatu. Nakon što je transakcija autorizirana od strane izdavatelja (D) korištenjem mreže, izdavatelj plaća trgovačkoj banci (C) određeni iznos jednak vrijednosti transakcije, odbijajući porez naplate, te ispisuje transakciju na korisnički račun. Trgovačka banka plaća iznos kupnje s neto popustom trgovcu. Trgovački popust, uz ostale stvari, uzima u obzir cijenu naknade transakcije, [33].

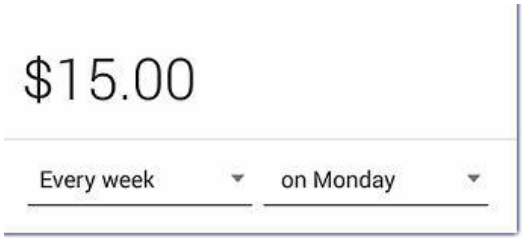
4.4. Dodatne značajke i funkcionalnosti

Dodane značajke aplikacije su upozorenje na nisko stanje računa koje služe za izbjegavanje neugodnih situacija prilikom plaćanja u slučaju da ostanete bez novca. Kad novac se spusti ispod određene granice, korisnik dobije obavijest o maloj razini novca, odnosno o stanju računa. Korisnik nakon ulaska u postavke mora odabrati opciju da želi primati obavijesti , te potom mu se nudi mogućnost odabira iznosa za koji želi da mu bude granica. Nakon odabira željenih postavki korisnik treba isto spremiti s pritiskom na dugme za povratak, [34].



Slika 4.9. Postavke za odabir obavijesti upozorenja, [34].

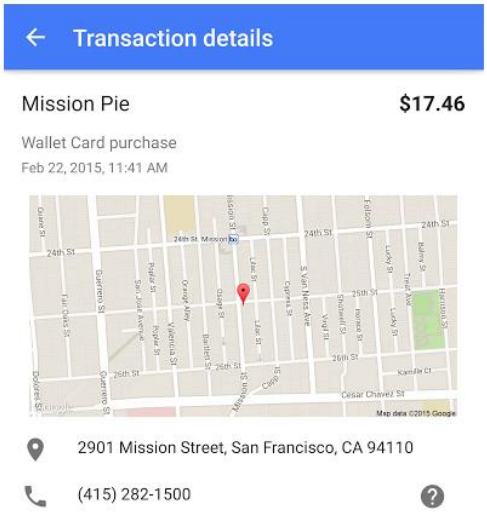
Još jedna korisna dodana značajka je mogućnost automatskog punjenja računa. Korisnik ima mogućnost uključivanja te opcije prilikom dodavanja novca na Google račun. Ova opcija je korisna jer korisnik ne mora brinuti o stanju računa, te je pogodna za korisnike koji imaju česte rashode, odnosno velike troškove. Račun se automatski puni na određeni datum, koji određuje korisnik, [34].



Slika 4.10. Korisnik odabire ponavljajući datum, [34].

Aplikacija je dobila nadogradnju 2013. godine s kojom se omogućuje slanje sredstava bilo kojoj punoljetnoj osobi koja posjeduje adresu elektroničke pošte, te je dostupna samo američkim korisnicima. Opcija slanja je besplatna kada se šalje s bankovnog računa ili Google Wallet servisa, no postoji mala naknada kada se koristi povezana kreditna ili debitna kartica. Korisnici koji šalju novac preko Google – ovog servisa dobiju rani uvid u buduću funkciju koja će biti implementirana u Gmail.

Riječ je o slanju novčanih sredstava direktno na desktopu iz Gmail - a. Unaprijeđena je podrška za sve kreditne i debitne kartice koje se mogu direktno učitati u Google Wallet aplikaciju, što eliminira potrebu za nošenjem plastičnih kartica sa sobom. Također unutar aplikacije sada mogu biti sačuvane razne ponude s Google Maps - a, društvene mreže Google+ i servisa Google Offers te ih se onda može platiti putem Google Wallet - a, [35].

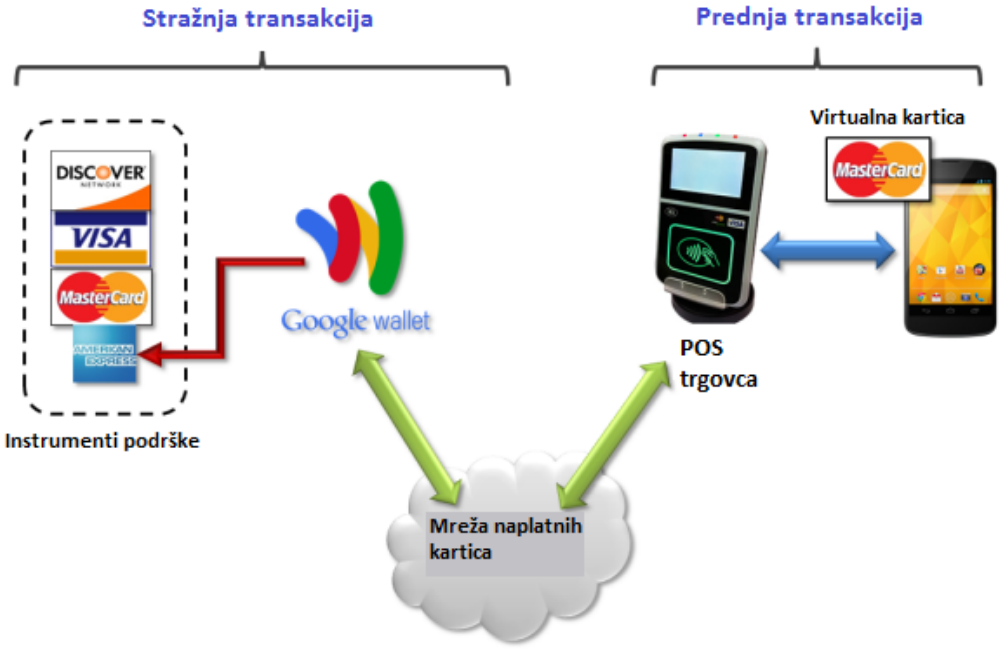


Slika 4.11. Prikaz karte obavljenih transakcija, [36].

Godine 2015. se pojavila nova značajka koja uključuje prozor karte koja pomaže korisnicima prikazati na karti gdje su obavljene sve transakcije. U idealnom slučaju, nova nadogradnja će funkcionirati kao sigurnosna mjera. Pogrešna ili slučajna transakcija će se prikazati očitom kada se nacrta na karti. S tim dodacima također dolaze i mane, Google Wallet ne koristi više svoj zadani zaslon. S ovom integracijom, korisnik ima uvid gdje je obavio pojedinu transakciju na karti. Ova značajka će pojednostavniti da se primijeti bilo kakva sumnjiva aktivnost koja se može pojaviti, [36].

4.5. Arhitektura Google Wallet platforme

Google Wallet uzima drukčiji pristup podržavajući više kartica u mobilnom novčaniku. Umjesto nošenja svih predstavljajućih instrumenata naplate, oni su svi skriveni iza „virtualne kartice“ koja može učinkovito preusmjeriti transakcije na bilo koju od originalnih kreditnih kartica. Usmjeravanje se obavlja u stvarnom vremenu preko mreže za naplatu, umjesto da pokušava stvoriti bitovne klonove kartice, [37].



Slika 4.12. Prikaz arhitekture Google Wallet-a i virtualnih kartica, [37].

Slika iznad prikazuje kako virtualne kartice funkcioniraju, u kontekstu mobilnog plaćanja korištenjem Android mobilnog uređaja preko NFC-a. Korisnici imaju jedan ili više pratećih instrumenata ili izvora financiranja u svom novčaniku. To su standardne kreditne kartice dodane konceptualnom novčaniku jednom utipkavajući broj kreditne kartice i druge relevantne detalje kao što su datum isticanja i „CVC2"[34] na web stranici ili mobilnoj aplikaciji. U bilo kojem trenutku, točno jedan od pratećih instrumenata naplate je aktivan, što znači da će se transakcija izvršiti s kartice. Isto kao i „*Coin*“, Google Wallet aplikacija ima korisničko sučelje za označivanje između opcija, [37].

[34] **CVC2** – Card Verification Code je sigurnosna šifra, trocifreni broj koji se nalazi na poleđini kartice.

Dok se Google Wallet koristi za pohranu NFC kupovine, kreditne kartice viđene od POS terminala nisu ni jedna od stvarnih pratećih instrumenata. Umjesto toga postoji virtualna kartica, jedinstvena u tom slučaju Google Wallet platforme. Svaki korisnik, pa čak i svaki primjer Wallet aplikacije povezane s određenim korisnikom ima vlastitu opremu virtualne kartice. U jednom smislu, ova kartica je vrlo realna. Radi se o punopravnoj MasterCard kartici izdanoj u ime Google-a, prihvaćena na bilo kojem NFC terminalu koji podržava MasterCard PayPass protokol. Radi se o običnom 16 – znamenkastom digitalnom broju kartice s prefiksom povezanim s MasterCard mrežom, datumom isteka i za NFC transakcije te kriptografske ključeve korištene za generiranje dinamičkog CVC[35] – a, [37].

Virtualna je u smislu da njezino postojanje nije izričito vidljivo. Primjerice, danas u mobilnim aplikacijama postoji broj kartice ili drugi detalji koji pripadaju korisniku, iako se često mogu primijetiti da su zadnje 4 znamenke otisnute i vidljive na računu. Zbog toga se nikad direktno ne upravlja od strane krajnjeg korisnika, niti se ne pojavljuje na potrošačkom izvješću o stanju računa kao dodatna kartica, [37].

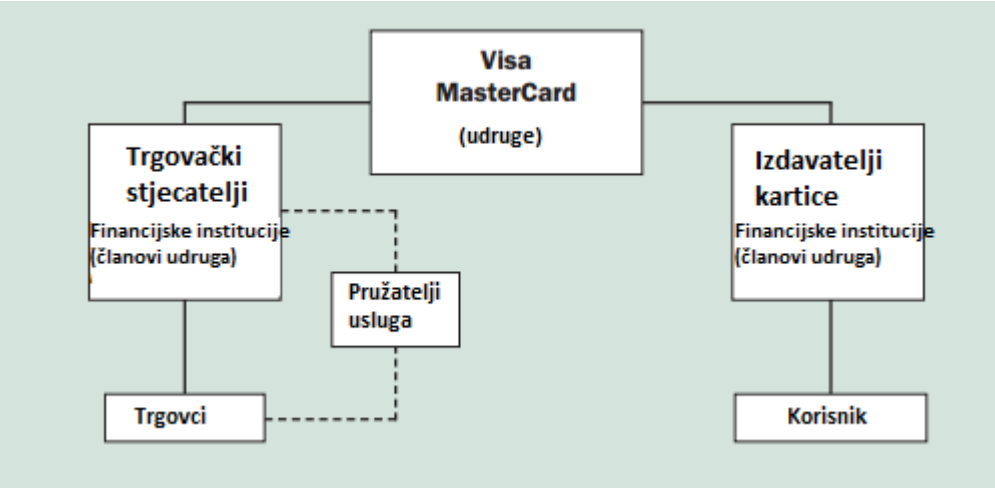
Kad korisnik izvršava NFC transakciju s Google Wallet-om, platna mreža (u ovom slučaju MasterCard) će odrediti put autorizacijskog zahtjeva prema Google-u, nominalnom izdavatelju virtualne kartice. Google će postaviti zahtjev za isplatu na aktivnu karticu s točnim istim iznosom. Ovisno o ishodu autorizacije, originalna „*front end*“ transakcija će biti odobrena ili odbijena. Sve je to učinjeno u realnom vremenu, te mora se završiti u roku od nekoliko sekundi u skladu s mrežnim pravilima o krajnjim rokovima transakcija, [37].

Postoje zanimljive posljedice ovog dizajna. Prva je ta da Google igra dvije uloge:

- Izdavatelj: Sve dok je trgovac u pitanju, Google je izdavatelj za karticu koju korisnik koristi. (Nominalno Google partneri s bankom za tu namjenu).
- Trgovac: Sve dok je originalni izdavatelj kartice u pitanju, Google je trgovac koji zahtjeva autorizaciju naplate kroz tu karticu, [37].

[35] **CVC** – je dodatna sigurnost na kreditnoj kartici u obliku broja koji služi za zaštitu od prijevara

Drugo zapažanje je da su virtualna kartica i stvarni prateći instrumenti potpuno razdvojeni. Za razliku od „*Coin*“ slučaja, Google Wallet virtualna kartica nije savršena replika originalne kartice koju korisnik dodaje u svoj novčanik. Nema isti datum isteka, ne dijele isto ime: za NFC transakcije, imena korisnika kartice su uređena. Zapravo, oni ne moraju biti na istoj mreži: Virtualne kartice su „MasterCard“, dok aktivni izvor financiranja mogu biti „Discover“ ili „American Express“ kartice, čak i ako trgovac ne prihvaća American Express kartice, uobičajena situacija kod malih poduzetnika. Trgovac s druge strane može biti malo bolji u smislu transakcijske naknade. Čak i ako prihvaćaju American Express, oni će vjerojatno platiti nižu naknadu za obradu transakcija za procesiranje istog iznosa preko MasterCard mreže, [37].

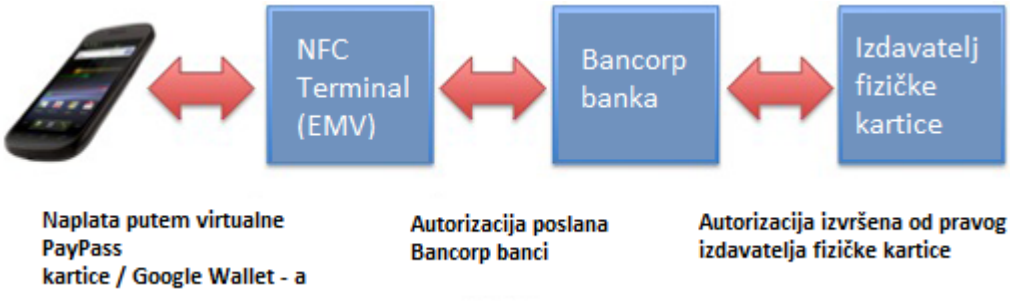


Slika 4.13. Stranke uključene u kartični program, [38].

Bitna stavka kod izvršenja naplate je komunikacija s bankom. Prilikom dodavanja osobnim podataka na kreditnu karticu (ime, broj, CVC, datum isteka), Google prosljeđuje te informacije na banku. Banka potom otvara virtualni račun, te radi dvije stvari: izdaje virtualnu beskontaktnu PayPass karticu koji zatim šalje OTA[36] u sigurnosni element uređaja. Osobni podaci naplate su povezani s tim računom, [39].

[36] **OTA** – Over The Air – pojam koji se često odnosi na usluge na koje se može pristupiti mobilnom uređaju bez potrebe za USB kabelom ili lokalnom Bluetooth vezom.

Ako se Google Wallet koristi za naplatu na *Point Of Sale* terminalu i odabire virtualne kartice, financijska institucija šalje zahtjev terminala u banke. Banka jednostavno prosljeđuje zahtjev izdavatelju realne kartice koji potom prenosi odgovor. Banka preuzima ulogu opunomoćenika koji usmjerava komunikaciju ispravnom izdavatelju kartice, [39].

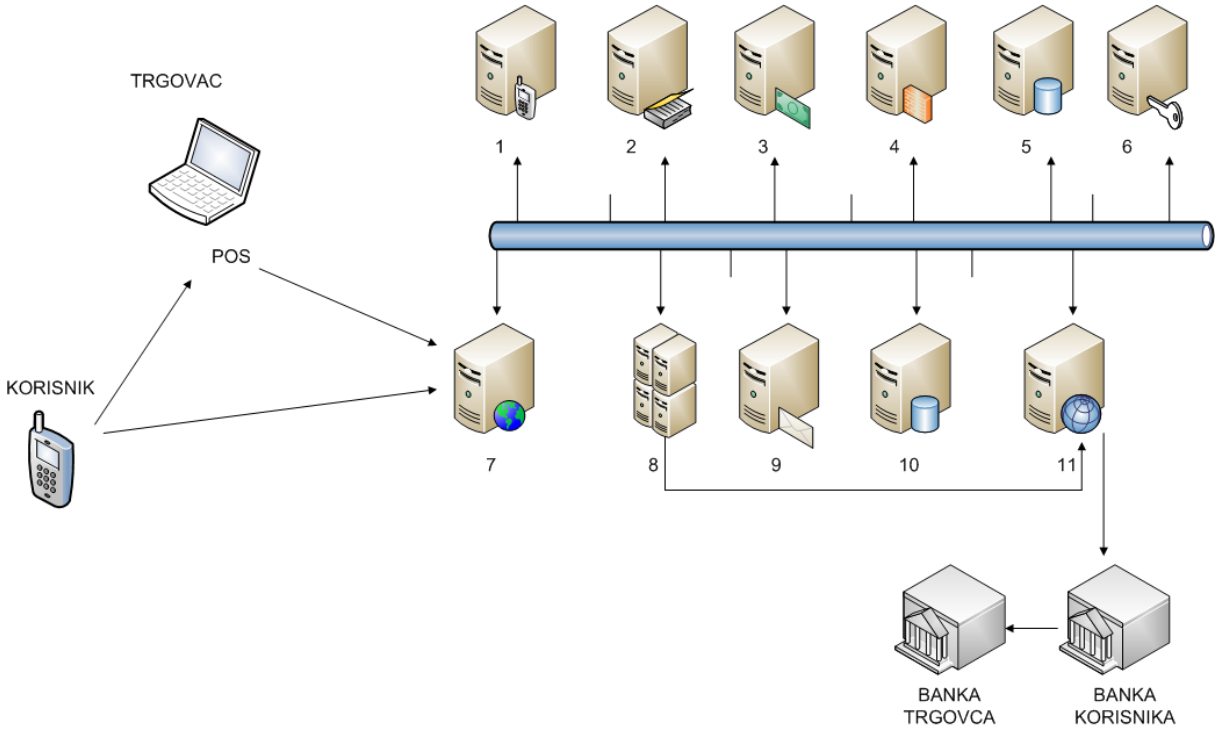


Slika 4.14. Princip komunikacije prilikom naplate, [39].

Postoje dvije kategorije elektroničkog novčanika:

- Elektronički novčanik poslužiteljske strane
- Elektronički novčanik klijentske strane

Elektronički novčanik poslužiteljske strane pohranjuje informacije o korisniku na udaljenom serveru pripadajući određenom trgovcu ili izdavatelju novčanika. (npr. Kad korisnik unese svoje informacije na „Amazon.com“, te informacije će biti pohranjene na poslužiteljskoj strani elektroničkog novčanika. Elektronički novčanik klijentske strane pohranjuje informacije na klijentskom računalu. Prednosti su da su osjetljive informacije pohranjene na korisničkom računalu umjesto centralnom serveru. Dok su nedostaci da se mora skinuti softver za svako računalo, te nije prijenosno, [39].



Slika 4.15. Prikaz arhitekture Google Wallet platforme (Visio)
Izvor:[40]

Tumač znakova:

- 1 – Sigurnosni server za upis
- 2 – Aktivni Microsoft server direktorija
- 3 – Autentifikacijski server
- 4 – Server za prijavu
- 5 – Registracijski server
- 6 – Certifikacijski server
- 7 – Portal
- 8 – Aplikacijski serveri
- 9 – e-mail / SMS server
- 10 – Server baze podataka
- 11 – „Gateway“ za naplatu

U trenutku kad se započne transakcija, pojave se dva glavna procesa: kartica se autorizira, te je transakcija nakon toga čista. Terminal šalje trgovcu identifikacijski broj, informaciju kartice i iznos transakcije prema procesoru kartice. Procesorski sustav čita informaciju i šalje autorizacijski zahtjev specifičnoj izdavačkoj banci preko kartične mreže. Izdavačka banka provodi niz provjera za prijevaru i ovjerava da je korisnikov iznos na računu dovoljan za pokriće kupovine prije povratka odgovora, bilo to odobreno ili odbijeno. Banka trgovca prima odgovor i prenosi ga trgovcu, [38].

Jednom kad je kartica autorizirana, drugi dio transakcije se izvršava, ili nabavlja proizvode korisniku i šalje novac na banku od trgovca. Trgovac šalje transakcije u banku trgovca, te potom banka šalje te informacije trgovačkom računovodstvenom sustavu. Trgovački računovodstveni sustav distribuira transakcije prema odgovarajućoj mreži (npr. Visa transakcije prema Visa mreži). Te potom odbija naknadu za odgovarajućeg trgovačkog popusta (da bi pokrio troškove aktivnosti banke trgovca) od transakcijskog iznosa.

Ovaj sustav je kompliciran, te sve više je na meti prevaranata, posebno kad su informacije o kartici spremljene na trgovački terminal ili poslane na nesiguran način. CNP[37] transakcije su manje sigurne nego transakcija u kojima se koriste kartice, zbog toga CNP transakcije zahtijevaju veće naknade za razmjenu od trgovca. Ali, iako NFC transakcije na Google Wallet platformi ne trebaju fizički prisutnu karticu, oni prenose informaciju kao da je kartica prisutna, pa naknade nisu visoke za trgovce koji su odabrali NFC na svom terminalu (POS), [38].

[37] **CNP** – Card Not Present

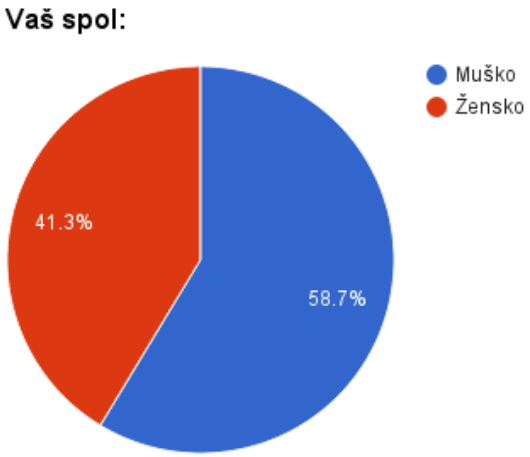
5. Analiza korisničkog iskustva korištenja usluga elektroničkog plaćanja

U ovom poglavlju diplomskog rada istražilo se preko anketnog upitnika korisničko iskustvo korištenja telekomunikacijskih usluga elektroničkog plaćanja. Anketa je bila provedena od 14. kolovoza do 8. rujna 2015. godine preko društvenih mreža (Facebook). U anketnom upitniku se istražilo trenutno stanje i vlastita iskustva korištenja telekomunikacijskih usluga u funkciji elektroničke naplate, te koja je vrsta elektroničke naplate najzastupljenija. Kroz pitanja se ispitala mogućnost prelaska na neke nove usluge, te korisničko osobno povjerenje u sigurnost elektroničke naplate.

Anketni upitnik se sastojao od 28 pitanja i bio je proveden nad uzorkom od 104 osobe preko Facebook društvene mreže. Prva pitanja su bila demografske prirode, te se potom prešlo na konkretna pitanja vezana za telekomunikacijske usluge elektroničke naplate. Početna pitanja vezana za usluge elektroničke naplate su bila orijentirana na učestalost korištenja elektroničkog plaćanja, prvotno da li se takva usluga koristi. Ispitanici su daljnjim pitanjima trebali obrazložiti zašto koriste ili ne koriste istu, te da li su zadovoljni uslugom elektroničke naplate. Sljedeća pitanja su provjeravala ispitanike da li su ikad čuli za NFC i Google Wallet usluge, te da li bi ih voljeli koristiti. Daljnja pitanja su bila sigurnosno koncipirana, tj. provjeravalo se da li su ispitanici ikad imali neke sigurnosne incidente, te da li imaju povjerenja u takve usluge.

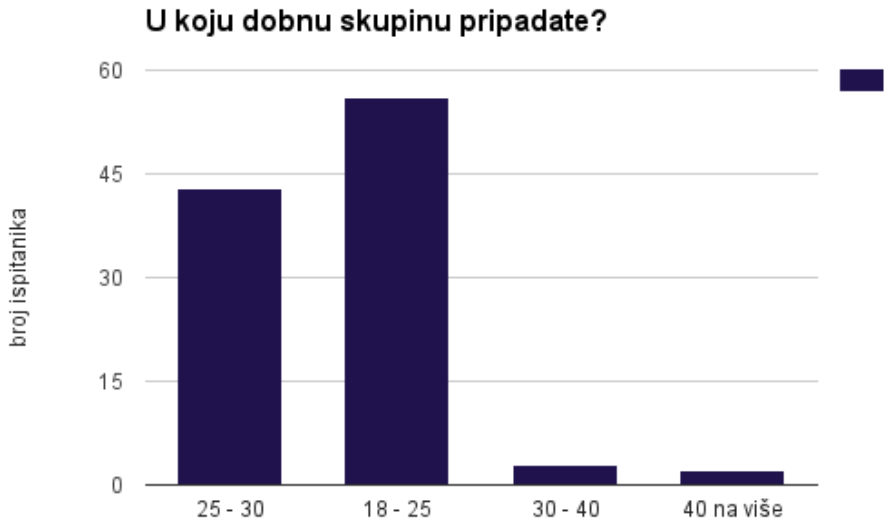
U anketnom upitniku, nakon pitanja mobilne naplate (Mpay) prešlo se na elektronički novac, te naplatu preko Interneta (Ipay). Pitanja su bila koncipirana tako da prikažu povjerenje i sigurnost u usluge naplate preko Interneta, te učestalost korištenja takvih usluga. Ciljalo se na primarne razloge korištenja naplate preko Interneta, koje se web stranice koriste za te usluge i mišljenja o sigurnosti usluga naplate preko Interneta. Ispitanici su imali mogućnosti obrazložiti o kakvom se sigurnosnom propustu radilo ako ga je bilo. Krajnja pitanja su bila orijentirana na prikaz mišljenja o postojećoj razvijenosti elektroničke naplate u Republici Hrvatskoj, te potom i na zadovoljnost dostupnošću takvih usluga, te na uočene mane ili negativnosti prilikom korištenja istih. U prilogu na kraju diplomskog rada su anketna pitanja, poslagana po redu kakva su bila u anketi.

Po pitanju spola 61 ispitanika se izjasnilo sa „muško, dok se 43 ispitanika izjasnilo sa „žensko“. Na slici ispod je vidljiv graf na kojem je u postotcima muških osoba 58.7%, te 41.3% ženskih osoba.



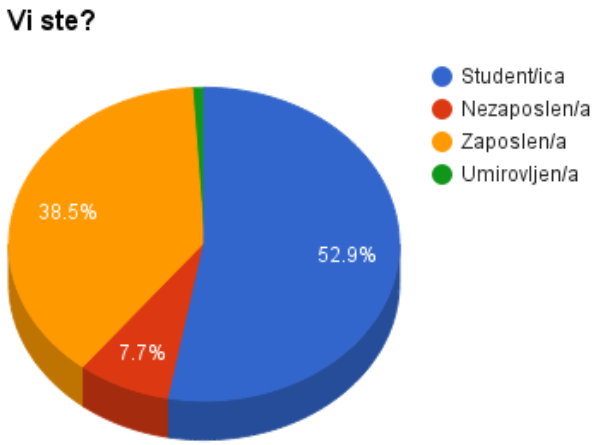
Grafikon 1. Opredjeljenje prema spolu

Najveći broj ispitanika je u dobnoj skupini od 18 do 25 godina sa 53.8%, po tom pitanju se izjasnilo 56 ispitanika. Od 25 do 30 godina je 41.3% ispitanih ljudi, odnosno 43 osobe. Od 30 do 40 godina su zaokružile 3 osobe, odnosno 2.9%, te 2 osobe su starije od 40 godine sa 1.9% ispitanika.



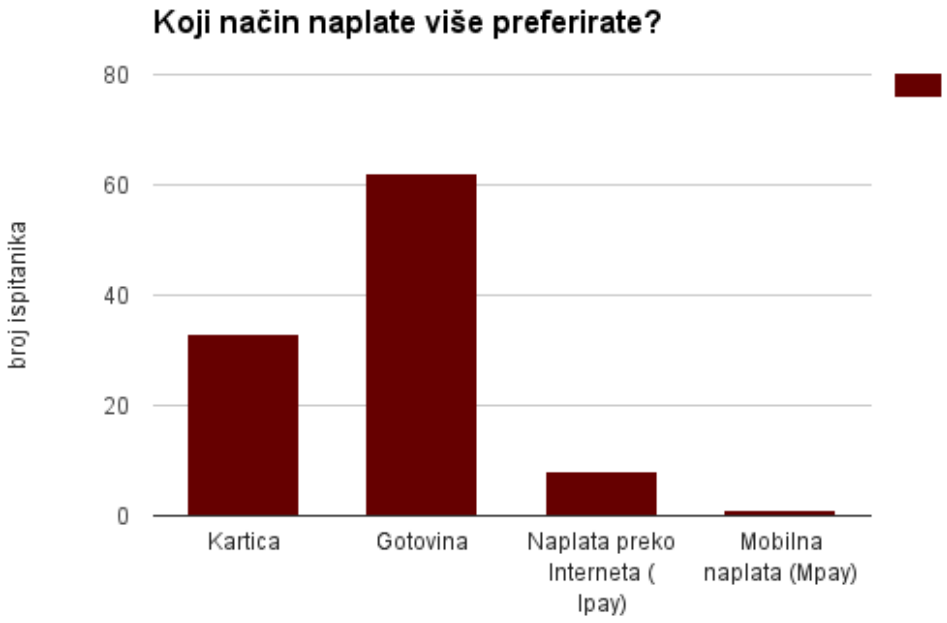
Grafikon 2. Dobna skupina

Od 104 ispitanih osoba, čak 55 (53.9%) se izjasnilo da su studenti, a 40 (38.5%) zaposlenih. Ostali su bili nezaposleni (7.7%), odnosno 8 osoba, dok je samo 1 osoba potvrdila da je umirovljena.



Grafikon 3. Prikaz statusa ispitanika

Većina anketiranih osoba najviše preferira naplatu gotovinom (59.6%), dok njih 31.7% preferira kartično plaćanje. Ostali ispitanici su se izjasnili za naplatu putem Interneta (7.7%), dok za naplatu preko mobilnog uređaja se izjasnila samo jedna osoba.

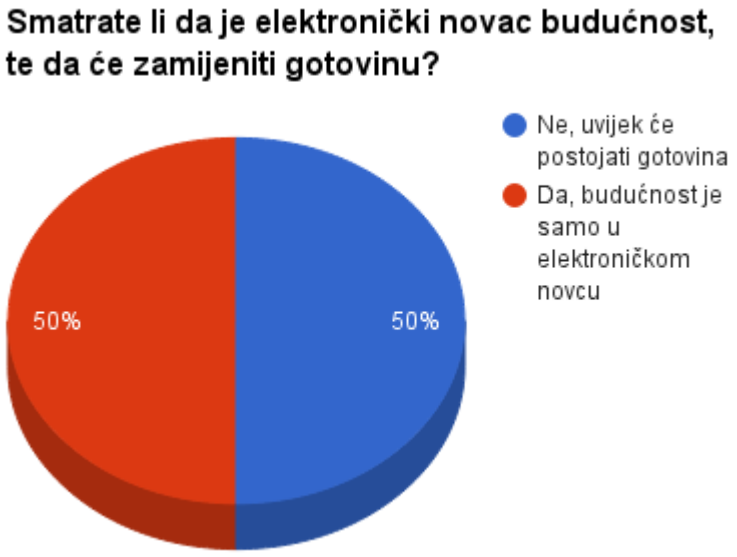


Grafikon 4. Preferirani način naplate

Na pitanje o elektroničkom novcu, 45 (43.3%) ispitanika se izjasnilo da je koristilo elektronički novac, 53 osobe su potvrdile da nisu koristili, dok 6 osoba nikad nije čulo za elektronički novac. Po pitanju da li smatraju da je elektronički novac budućnost, te da će u potpunosti zamijeniti gotovinu, 50 % ispitanika je odgovorilo da hoće.

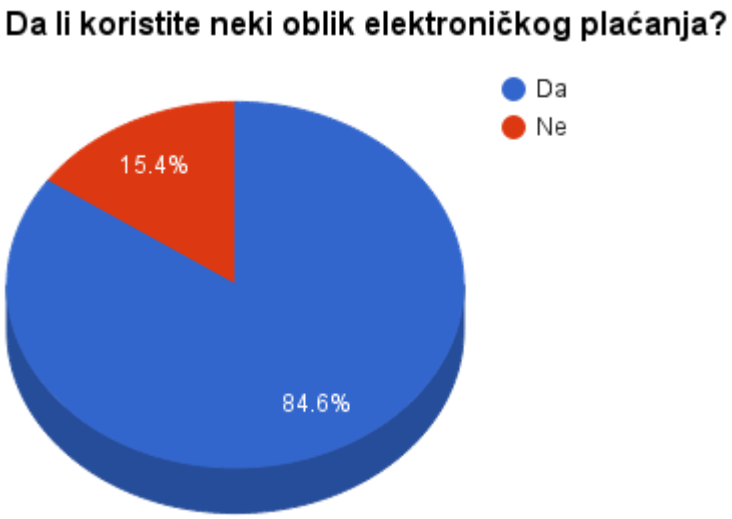


Grafikon 5. Prikaz stope korištenja e - novca

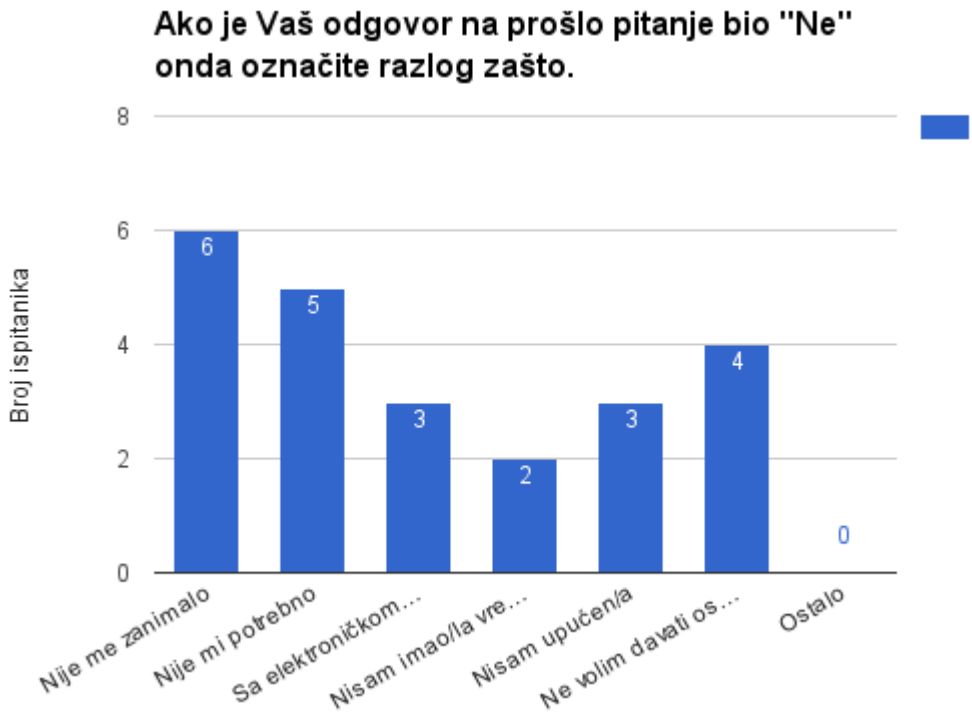


Grafikon 6. Pitanje o mišljenju da li e - novac budućnost

Veći dio ispitanika, njih 84.6% je na pitanje da li koriste neki oblik elektroničkog poslovanja odgovorilo sa „Da“, dok je ostatak od 16 osoba odgovorio sa „Ne“. Pitanje je slijedilo potpitanja s kojim se doznao razlog zbog čega tih 16 osoba nije nikad koristilo neki oblik elektroničkog plaćanja.

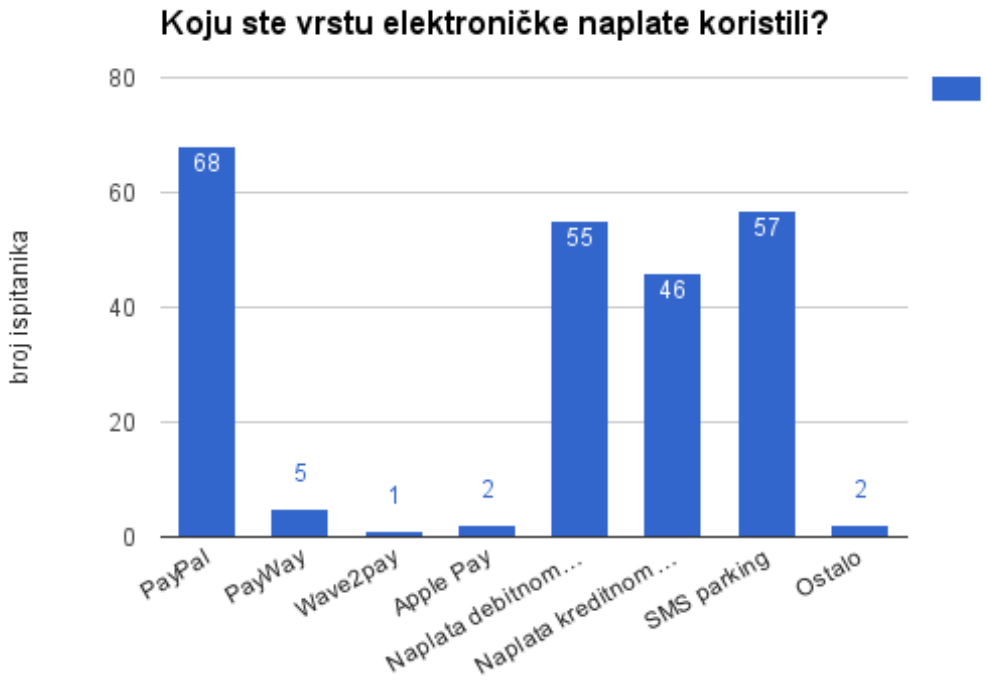


Grafikon 7. Oblik elektroničkog plaćanja



Grafikon 8. Pitanje o definiranju razloga zašto "Ne

Većina ljudi koji nisu koristili elektroničku naplatu se izjasnilo da je to zbog toga što ih nije zanimalo (33.3%), dok je 27.8% ispitanika potvrdilo da im nije bilo potrebno. Njih 16.7% smatraju da im je s elektroničkom naplatom ugrožena sigurnost. Za elektroničku naplatu nisu imali vremena 11.1% ispitanih osoba, dok 16.7% nije upućeno u funkcionalnost elektroničke naplate. Od ukupnog broja ispitanih osoba koje nisu nikad koristile usluge elektroničke naplate, njih 22.2% tvrdi da je to zato što ne volu davati osobne podatke na Internet.



Grafikon 9. Vrsta elektroničke naplate koja se koristi

Od ispitanih osoba koji su se koristili elektroničkom naplatom, većina sa 71.6% (68 ispitanika) je odgovorilo da se služilo s PayPal uslugom elektroničke naplate. Nešto manje, odnosno 60% ispitanika je koristilo uslugu SMS parkinga, dok je 57.9% ispitanika koristilo naplatu debitnom karticom. Naplatu kreditnom karticom je koristilo 48.4% ispitanih osoba, a 5 osoba je koristilo PayWay i samo jedna osoba je potvrdila da je koristila Wave2Pay uslugu elektroničke naplate. Apple Pay uslugu od tvrtke Apple su potvrdile 2 osobe, te ostale načine naplate su odabrale 2 osobe.

Po pitanju zadovoljstva s uslugom elektroničke naplate, 98% ispitanika je potvrdilo da je zadovoljno, odnosno 2% da nije zadovoljno s istom. Sljedeće pitanje je tražilo od ispitanika da se ukratko izjasne zašto nisu zadovoljni. Jedna osoba je potvrdila da je razlog nezadovoljstva kontrola troškova, te upitna sigurnost. Druga osoba se izjasnila da je ponekad još uvijek kompliciran s upotrebom tokena, te smatra da novi sustavi s naplatom na kontakt olakšavaju krađu jer ne zahtijevaju PIN.



Grafikon 10. Zadovoljstvo sa uslugom elektroničke naplate

Sljedeće pitanje je provjerilo da li ispitanici koriste mobilni uređaj koji podržava NFC tehnologiju. Na to pitanje 56.7% ispitanih osoba je potvrdilo da ne koriste, dok ostatak od 43.3% osoba se izjasnilo da koriste uređaj koji podržava NFC tehnologiju.

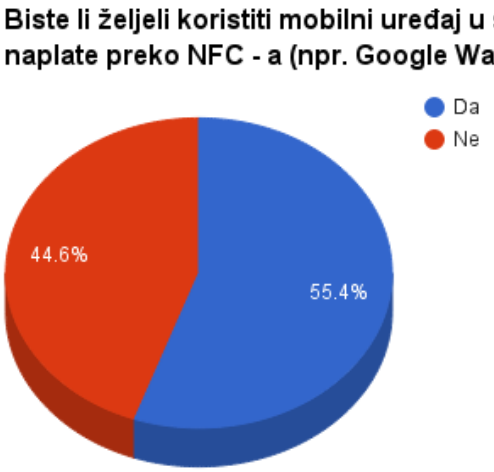


Grafikon 11. Korištenje uređaja koji podržava NFC

Nadalje, kroz sljedeća pitanja se željelo saznati upoznatost s Google Wallet uslugom elektroničke naplate, te zainteresiranost u istu. Većina ispitanika, njih 57.7% je potvrdila da nije nikad čula za Google Wallet. Dok većina od 41 ispitanika (55.4%) koji su upoznati s Google Wallet uslugom, bi istu željeli i koristiti.

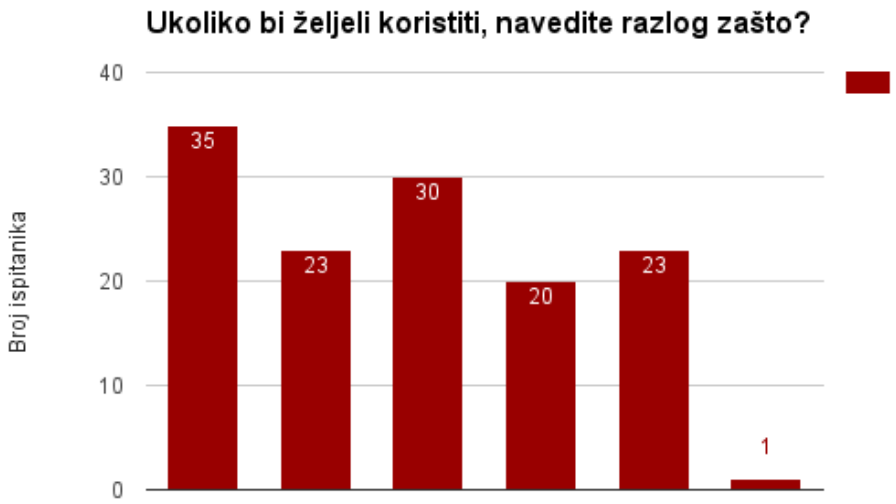


Grafikon 12. Postotak ispitanika koji su čuli za uslugu "Google Wallet"



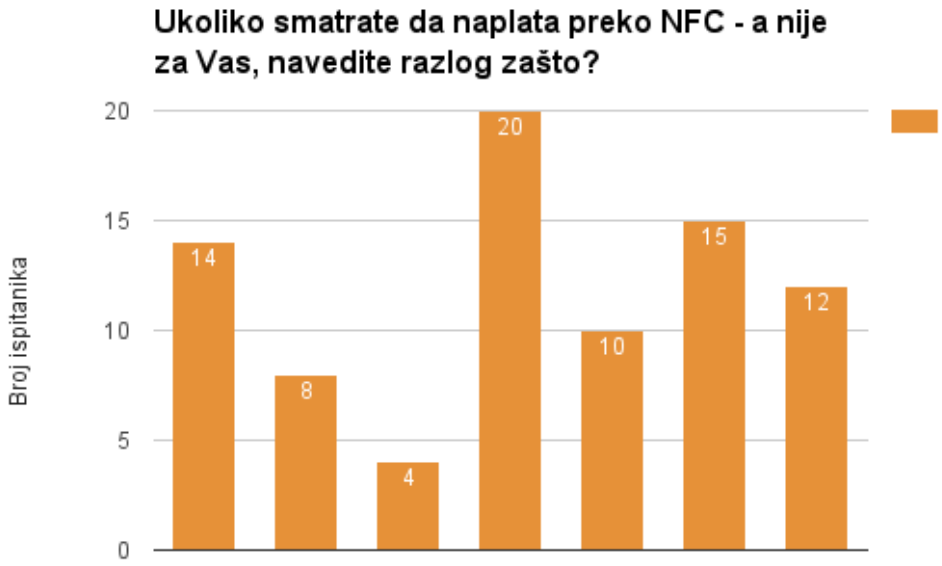
Grafikon 13. Pitanje o zainteresiranosti za Google Wallet uslugu

Pitanje o zainteresiranosti za Google Wallet uslugom sljedilo je pitanje da se navede razlog zašto bi ispitanici željeli koristiti istu uslugu. Najviše je ispitanika (35 glasova) s 63.6% potvrdilo da je razlog jednostavna naplata, iza toga slijedi odgovor za uštedu vremena na blagajni s 54.5% (30 osoba). 23 osobe su se izjasnile da je razlog jer ne trebaju imati gotovinu uz sebe, 20 osoba smatra da s tom uslugom bi imala potpuni pregled povijesti naplate, te 20 osoba voli biti u skladu s tehnologijom.



Grafikon 14. Pitanje o razlogu zašto bi ispitanici željeli koristiti uslugu NFC naplate

Isto tako, osobe koje nisu zainteresirane za naplatu preko NFC – a, su imale priliku se izjasniti zašto su pri tom mišljenju. Većina s 20 glasova, odnosno 38.5% se boji neovlaštenog korištenja mobilnog uređaja, dok 15 osoba s 28.8% nema nikakve potrebe za tim. 14 osoba s 26.9% nema osjećaj koliko troši, te 10 ispitanika je naviklo samo na gotovinsku naplatu. Ostatak osoba smatra da takva usluga nije još dovoljno sigurnosno razvijena da bi je koristili, a 4 osobe nemaju povjerenja u elektronsku naplatu. Pod rubriku „Ostalo“ je dalo svoj odgovor 12 osoba, ali se nisu izjasnili.

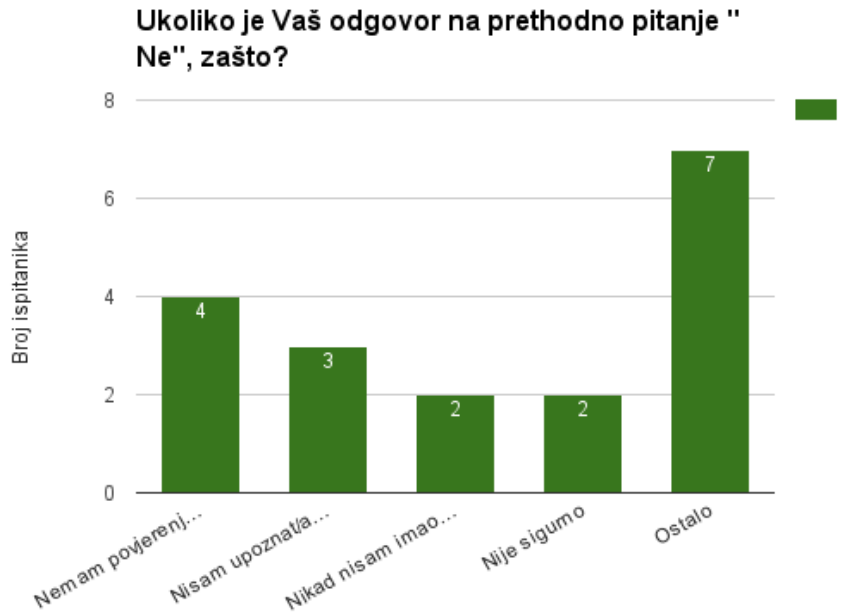


Grafikon 15. Pitanje o razlogu zašto ne bi željeli koristiti uslugu NFC naplate

Pitanja koja slijede su bazirana na Internet plaćanjima, željelo se doznati od ispitanika da li kupuju preko Interneta, te razloge zašto kupuju, odnosno zašto ne kupuju. Od ukupnog broja ispitanika, 85.6% je odgovorilo da kupuju preko Interneta, dok ostatak od 14.4% ne kupuje. Od ispitanika koji ne kupuju preko Interneta, kao razlog zašto ne kupuju najčešće je bio pod rubrikom ostalo, ali se nisu izjasnili zašto (43.8%). Zatim slijedi 25% ispitanika koji nemaju povjerenja u transakcije preko Interneta, 18.8% ispitanih osoba koji nisu upoznati s kupnjom preko Interneta. 12.5% osoba nije imalo potrebe za Internet plaćanjima, dok 12.5% smatra da nije sigurno.

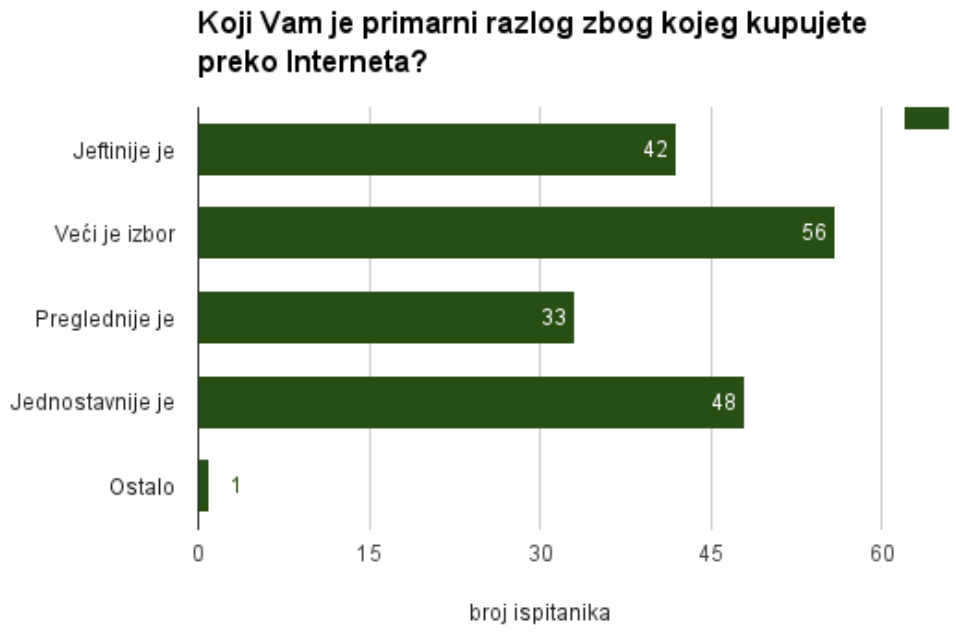


Grafikon 16. Postotak kupnje preko Interneta



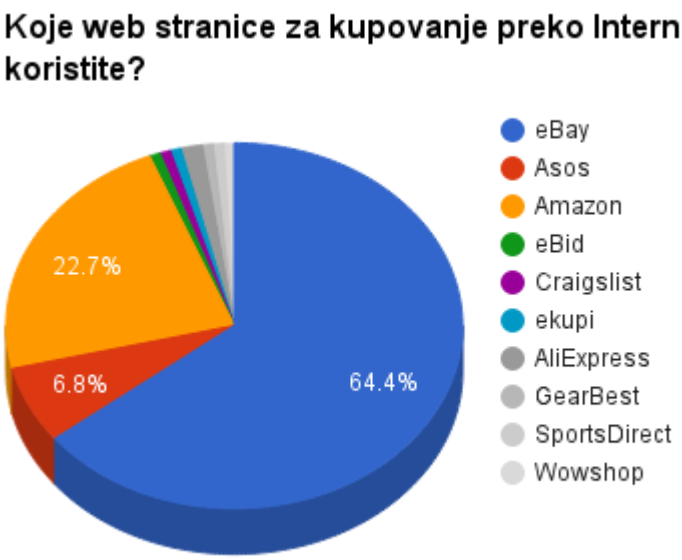
Grafikon 17. Razlog zašto se ne kupuje preko Interneta

Pod odgovore na pitanje da se navede razlog zašto se ne kupuje preko Interneta, 61.5% (56 osoba) odgovorilo je da je kupnjom preko Interneta veći izbor. 52.7% ispitanih osoba odgovorilo je da jednostavnije kupovati preko Interneta, 46.2% osoba se izjasnilo da je jeftinije, 36.3% osoba smatra da je preglednije, te 1.1% (jedna osoba) je odabrala rubriku „Ostalo“.



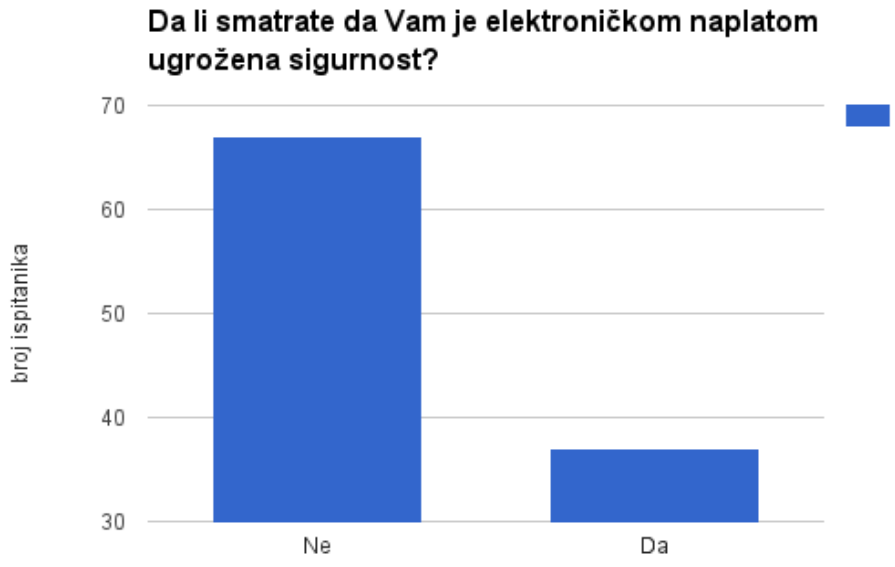
Grafikon 18. Razlog kupnje preko Interneta

Nadalje, po pitanju web stranica koje se koriste za kupovanje preko Interneta, 64.4% ispitanika se izjasnilo da koristi eBay, 22.7% koristi Amazon, 6.8% se koristi Asos stranicom, te Craigslist i eBid sa 0.8% svaki. Ostale stranice koje nisu navedene pod ponuđenim odgovorima je odabralo 4.5% ispitanika. U grafu na sljedećoj stranici je prikazano polje „Ostalo“ u nijansama sive boje, koje je podijeljeno u par definiranih stranica. Stranice koje je navela nekolicina ispitanika pod „Ostalo“ su: AliExpress s 2 glasa, GearBest s jednim glasom, SportsDirect s jednim glasom, te Wowshop s jednim glasom.



Grafikon 19. Web stranice koje se koriste za kupnju preko Interneta

Sljedeće pitanje je bilo orijentirano na sigurnost elektroničke naplate, postavilo se pitanje da li ispitanici smatraju da im je elektroničkom naplatom ugrožena sigurnost. Od ukupnih ispitanika, 64.4% je odgovorilo da im nije ugrožena sigurnost, a 35.6% ispitanika smatra da im je sigurnost ugrožena.



Grafikon 20. Mišljenje o sigurnosti elektroničke naplate

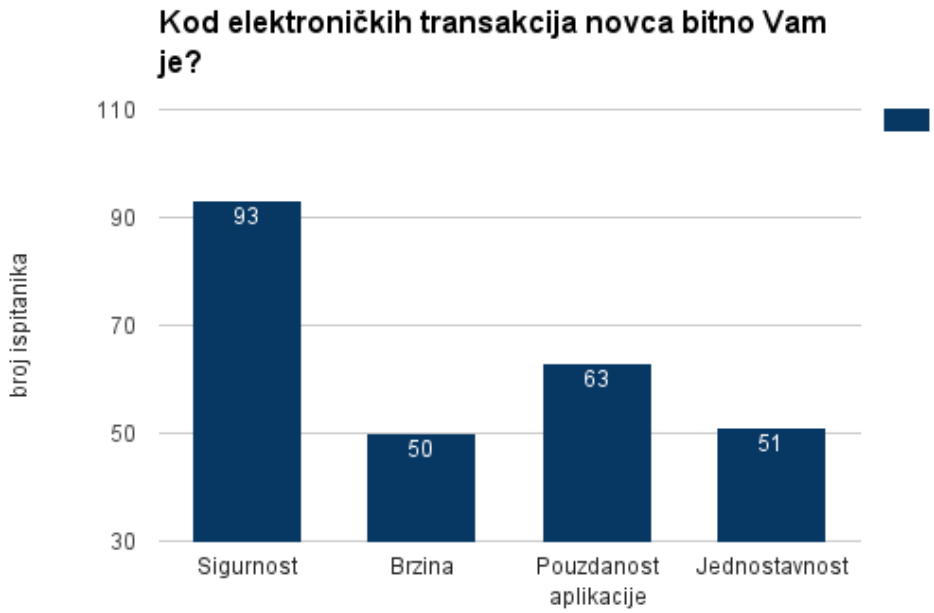
Nadalje, postavilo se pitanje da li su ispitanici ikad imali iskustva sa sigurnosnim propustom bilo koje vrste. Na ovo pitanje, 98.1% ispitanika je potvrdilo da nikad nisu imali iskustva sa sigurnosnim propustom, dok 1.9% (dvije osobe) su potvrdile da jesu. Osobama koje su imale iskustva sa sigurnosnim propustom se postavilo sljedeće pitanje iz kojeg je trebalo biti razvidno o kojim se sigurnosnim propustima radilo. Jedna osoba je odgovorila da joj je netko otuđio karticu i imao sve potrebne podatke na izvršenje naplate, te je banka vratila ukradeni novac. Druga osoba se izjasnila da joj je POS uređaj odbio karticu nekoliko puta, te artikl je ostao neplaćen. Iz ovoga možemo zaključiti da su sigurnosni propusti rijetki, ali ipak mogući, pogotovo danas dok je elektronička naplata u fazi razvoja, te dok se nisu eliminirale sve anomalije i propusti.



Grafikon 21. Iskustva sa sigurnosnim propustima

Sigurnosni propusti se ne smiju zanemarivati, treba se što više raditi na rješavanju tih problema, kako bi se umanjili gubici bilo koje vrste. Ovaj postotak dokazuje da je danas postala vrlo mala mogućnost da se neki sigurnosni propust dogodi. To je pozitivan rezultat rada na sigurnosti elektroničke naplate, te zbog toga sve veći broj korisnika ima povjerenja u takve usluge.

Na pitanje o tome što je korisnicima bitno kod elektroničkih transakcija novca, 93 ispitanih osoba (89.4%) odgovorilo je da im je bitna sigurnost. Nadalje, 60.6% osoba je bitna pouzdanost aplikacije, 49% jednostavnost, te 48.1% ispitanika je bitna brzina.



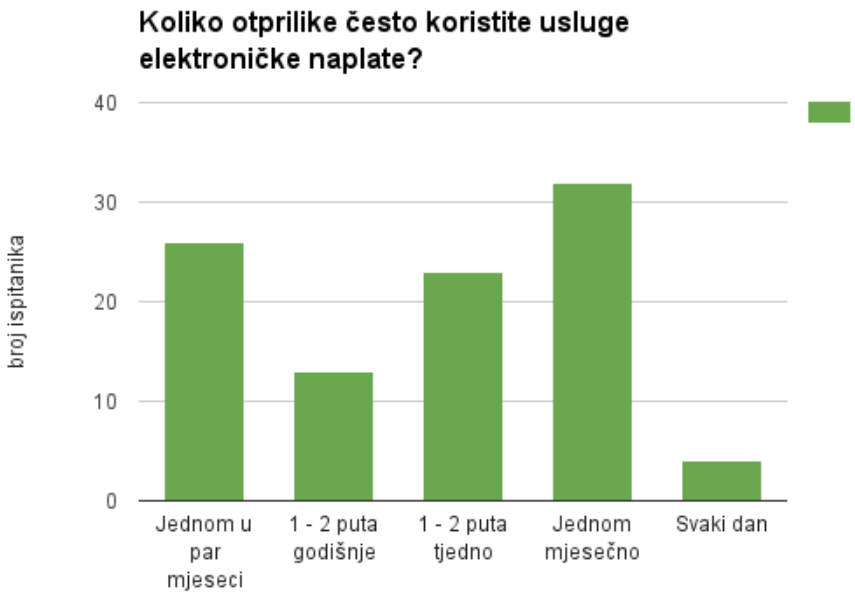
Grafikon 22. Pitanje o elektroničkim transakcijama

U sljedećem pitanju su ispitanici mogli ocijeniti prema vlastitom mišljenju trenutnu razvijenost elektroničke naplate u republici Hrvatskoj. Rezultati su sljedeći, 54.8% ispitanika smatra da je trenutna razvijenost dobra, 31.7% ispitanika smatra da je loša, te 13.5% ispitanih osoba smatra da je razvijenost vrlo dobra. Niti jedna od ispitanih osoba nije potvrdila da je razvijenost elektroničke naplate u republici Hrvatskoj odlična.



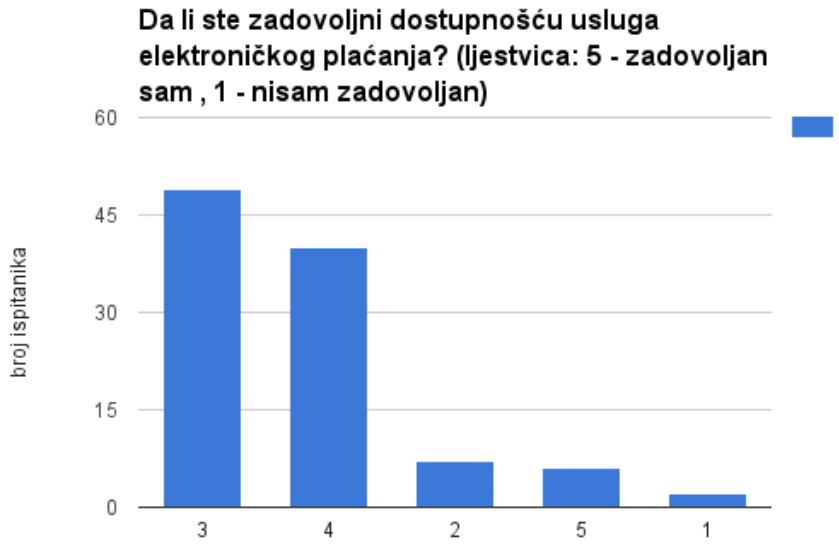
Grafikon 23. Vlastito mišljenje o razvijenosti elektroničke naplate u RH

Što se tiče pitanja o učestalosti korištenja usluga elektroničke naplate, većinski udio od 32.7% osoba ih koristi jednom mjesečno. Jednom u par mjeseci ih koristi 26.5%, a 23.5% osoba usluge koristi 1 – 2 puta tjedno. Usluge elektroničke naplate, 1 – 2 puta godišnje koristi 13.3% osoba, dok samo 4.1% osoba takve usluge koristi svaki dan.



Grafikon 24. Učestalost korištenja usluga elektroničke naplate

Prema predzadnjem pitanju o zadovoljstvu dostupnošću usluga elektroničkog plaćanja (na ljestvici od 1 do 5), 47.1% osoba je dalo ocjenu „3“. Iza toga slijedi 38.5% osoba s ocjenom „4“, 6.7% osoba je ocijenilo sa „2“, 5.8 % sa „5“, te 1.9% ispitanika s ocjenom „1“.



Grafikon 25. Zadovoljstvo dostupnošću usluga elektroničkog plaćanja

U zadnjem pitanju ovog anketnog upitnika se željelo doznati da li su ispitanici uočili neke negativnosti ili mane prilikom korištenja usluga elektroničke naplate. Na ovo pitanje su odgovorili samo ispitanici koji su uočili negativnosti, najveći broj sa 48.6% ispitanika se izjasnilo da imali problema s blokiranjem aplikacije za elektroničku naplatu. Nakon toga slijedi problem nestanka baterije na uređaju prilikom procesa naplate sa 35.1%, potom 24.3% ispitanika s nemogućnošću očitavanja NFC taga, te 10.8% s hakerskim napadom. Pod „Ostalo“ je glasala samo jedna osoba, ali se nije izjasnila točno o kojem se problemu radi.



Grafikon 26. Uočene negativnosti ili mane korištenja usluga elektroničke naplate

6. Zaključak

Usluge elektroničke naplate u svijetu su u uzastopnom rastu, imaju tendenciju poboljšanja sigurnosti i eliminiranja propusta. Razvojem Interneta došlo se do novih mogućnosti u platnom sustavu, te je potaknulo čovječanstvo da pređu na novi i moderniji način poslovanja. Prekretnica uz Internet je bio i razvoj kreditnih kartica, koje su u svom početku bila uvodna faza za elektroničko plaćanje, te su vrlo utjecale na promjenu načina poslovanja. Evolucijom elektroničkih tehnologija za naplatu se došlo do spoznaja novih tehnologija koje su doprinijele nove načine naplate. Razvoj kreditnih kartica je bio novi korak prema modernijim načinima naplate, potom su se počele razvijati nove tehnologije. Bitna faza razvoja elektroničke naplate je bila pojava elektroničkog novca, koji je postao dio modernog bankarstva, te se kao takav danas nastoji usavršiti u vidu korištenja i sigurnosti.

Na razvoj modernih tehnologija naplate i prijenosa novca utječu razni faktori (nove informacijsko komunikacijske tehnologije, internet itd.), te sve ovisi o stanju razvoja u jednoj državi. Rijetko se može naići na informacije koje potvrđuju moguću poziciju koju elektronički novac može imati u budućnosti, te kako korisnici vide cjelokupni proces korištenja elektroničkog novca. Upravo korisničko prihvaćanje je ključ za određivanje izvedivosti i učinkovitosti elektroničkog novca. Prekretnica elektroničke trgovine je bila pojava elektroničkog novčanika, koji omogućuje pojedincu da obavi transakcije elektroničke trgovine. Još uvijek je u razvoju, pa je stoga tema rasprava o sigurnosti i povjerenju korištenja istog. Korisnici su još uvijek skeptični prema elektroničkom vidu naplate, te je potreban određeni vremenski period da se postigne konzistentna zaštita osobnih podataka.

Analizom prikupljenih rezultata anketnog upitnika došlo se do spoznaja o načinima prihvaćanja novih tehnologija kod korisnika, te povjerenja u iste. U anketnom upitniku većina anketiranih osoba najviše preferira naplatu gotovinom, te većina nije upoznata s tehnologijom elektroničkog novca. Iz rezultata uzorka je vidljivo da razvijenost elektroničke naplate u Republici Hrvatskoj nije u skladu s ostalim Europskim zemljama. Svake godine elektronička naplata postaje sve više prihvaćen način plaćanja, te se predviđa da će u skoroj budućnosti biti preferirani način naplate. Isto tako, po pitanju da li smatraju da je elektronički novac budućnost, te da će u potpunosti zamijeniti gotovinu, 50 % ispitanika je odgovorilo da hoće.

Većina ispitanih osoba je koristila neki oblik elektroničke naplate, te čak 98% ispitanika je zadovoljno s korištenjem elektroničke naplate. Po pitanju o zainteresiranosti za „Google Wallet“ uslugu elektroničkog novčanika, više od pola ispitanih osoba je potvrdilo da je zainteresirano. Prema rezultatima analize anketnog upitnika, jednostavna naplata je najčešći razlog zašto ispitanici preferiraju elektronički novčanik. Kod ispitanika koji nisu zainteresirani za elektronički novčanik, najčešći je razlog strah od neovlaštenog korištenja mobilnog uređaja. Usluge elektroničke naplate se kod ispitanika najčešće koriste jednom mjesečno, dok se po pitanju zadovoljstva 47.8% osoba opredijelilo za srednju ocjenu „3“. Rezultati pokazuju da je razvijenost elektroničke naplate u Republici Hrvatskoj ocijenjena srednjom dobrom ocjenom. Blokiranje aplikacije za naplatu, uz nestanak baterije na uređaju su najčešći nedostaci kod ispitanika.

Prema rezultatima istraživanja ovog diplomskog rada, može se doći do zaključka da su korisnici elektroničke naplate zadovoljni s istom. Ipak, sudeći po rezultatima ankete, ispitanici nisu dovoljno zainteresirani za neke nove usluge (Google Wallet), te su skeptični po pitanju davanja osobnih podataka na Internet. Mobilni uređaj koji podržava NFC tehnologiju posjeduje 43.3% ispitanika, a većina ispitanih osoba nikad nije čula za Google Wallet. Ispitanici su više orijentirani prema naplati preko Interneta, dok je primarni razlog jednostavnost naplate i jeftinija kupnja. Među ispitanicima najviše se koriste „eBay“ i „Amazon“ web stranice. Po pitanju sigurnosti, većina ispitanika smatra da im nije ugrožena sigurnost i nije imala iskustva sa sigurnosnim propustima.

LITERATURA

[1] A. Dujella, M. Maretić, Kriptografija, Element, Zagreb; 2007

[2] Hauben R, A study of the ARPANET TCP/IP Digest and of the roll of the online communication in the Transition from the APRPANET to the Internet. [cited 2015 may]. Avaible from: http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt

[3] Hamm T, Edward Bellamy, Inventor of The Credit Card. [cited 2015 May]. Avaible from: http://www.thesimpledollar.com/a-fascinating-look-at-edward-bellamy-inventor-of-the-credit-card/

[4] The evolution of credit cards. [cited 2015 May]. Avaible from: http://www.bankrate.com/finance/financial-literacy/the-evolution-of-credit-cards-2.aspx

[5] Woolsey B, Starbuck Gerson E, The history of credit cards. [cited 2015 May]. Avaible from: http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php

[6] The evoulution of Electronic Payment. [cited 2015 May]. Avaible from: http://www.switchpay.com/evolution-electronic-payments/

[7] History of Mobile and Contactless Payment System. [cited 2015 June]. Avaible from: http://www.nearfieldcommunication.org/payment-systems.html

[8] History of Near Field Communication. [cited 2015 June]. Avaible from: http://www.nearfieldcommunication.org/history-nfc.html

[9] Rouse M, Biometric payment definition. [cited 2015 June]. Avaible from: http://searchsecurity.techtarget.com/definition/biometric-payment

[10] Emer M, Biometrija u bankama. [In Croatian]; [cited 2015 June]. Avaible from: http://zastita.info/hr/clanak/2011/9/biometrija-u-bankama-sve-cesce-rjesenje,198,6133.html

[11] The advantages of biometric payment system. [cited 2015 June]. Avaible from: http://www.biometric-security-devices.com/biometric-payment-system.html

[12] Hrvatska akademska i istraživačka mreža (CARNet), Elektronički novac. [In Croatian]; [cited 2015 June]. Netlibrary: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-09-311.pdf

[13] Slivonja M, Notacijski sustavi elektroničkog plaćanja. [In Croatian]; [cited 2015 June]. Avaible from: http://web.zpr.fer.hr/ergonomija/2004/slivonja/notacijski_sustavi_el_placanja.htm

[14] Slivonja M, Simbolički sustavi elektroničkog plaćanja. [In Croatian]; [cited 2015 June]. Avaible from: http://web.zpr.fer.hr/ergonomija/2004/slivonja/simbolicki_sustavi_el_placanja.htm

[15] Centralized Account Processing System (CAPS). [cited 2015 June]. Avaible from: https://www.usps.com/nationalpremieraccounts/accountoverview.htm

[16] Al Laham, M, Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy. [cited 2015 June]. Avaible from: http://iisit.org/Vol6/IISITv6p339-349Al-Laham589.pdf

[17] Popovska-Kamnar N, The Use of Electronic Money and Its Impact on Monetary Policy. [cited 2015 June]. Avaible from: http://www.eccf.ukim.edu.mk/ArticleContents/JCEBI/JCEBI_2/spisanie%20Neda%20Popovska-Kamnar.pdf

[18] Sova K, Electronic money trends [Bac. Thesis]. Turku University of Applied Sciences; 2013 [cited 2015 August]. Avaible from: https://www.theseus.fi/bitstream/handle/10024/54896/Sova_Kristina.pdf?sequence=1ž

[19] E-money trends. [cited 2015 August]. Avaible from: http://www.wrsc.org/attach_image/e-money-trends

[20] Athanassiou P, Mas-Guix N, Electronic money institutions. European Central Bank; 2008. [cited 2015 June]. Avaible from: https://www.ecb.europa.eu/pub/pdf/scplps/ecblwp7.pdf

[21] Nino Ž, Protokoli plaćanja elektroničkim novcem. Fakultet Elektrotehnike i Računarstva; 2002. [In Croatian]; [cited 2015 June]. Avaible from: http://os2.zemris.fer.hr/en/2002_zeljko/index.htm

[22] Početak Interneta i nastanak weba. [In Croatian]; [cited 2015 May]. Avaible from: https://element.hr/artikli/file/1259

[23] Electronic Money System Secutity Objectives, European Central Bank; 2003. [cited 2015 June]. Avaible from: http://www.dnb.nl/en/binaries/Electronic%20MoneySystemSecurityObjectives_tcm47-145657.pdf

[24] Blažević M, Sigurnost digitalnog identiteta i moguća rješenja autentifikacije, Digitalni potpis. Fakultet Elektrotehnike i Računarstva. [In Croatian]; [cited 2015 June]. Avaible from: http://web.zpr.fer.hr/ergonomija/2005/blazevic/oautoru.htm

[25] Blažević M, Sigurnost digitalnog identiteta i moguća rješenja autentifikacije, Digitalni slijepi potpis. Fakultet Elektrotehnike i Računarstva [cited 2015 June]. Avaible from: http://web.zpr.fer.hr/ergonomija/2005/blazevic/slijepi_potpis.htm

[26] Rouse M, Google Wallet definition [cited 2015 June]. Avaible from: http://searchcio.techtarget.com/definition/Google-Wallet

[27] What Google Wallet means. [cited 2015 August]. Avaible from: https://www.techopedia.com/definition/27518/google-wallet

[28] Google Wallet support, Google Wallet Fraud Protection, [cited 2015 July]. Avaible from: https://support.google.com/wallet/answer/6285573?hl=en&rd=1

[29] Sassi H., Google Wallet Purchase Scam. [cited 2015 July]. Avaible from: http://www.bbb.org/blog/2014/01/warning-google-wallet-purchase-scam/

[30] Google Wallet support, Introducing the new Google Wallet [cited 2015 July]. Avaible from: http://www.google.hr/wallet/

[31] Parker M, Media D, Is your Debit card information safe with Google Wallet. [cited 2015 July]. Avaible from: http://smallbusiness.chron.com/debit-card-information-safe-google-wallet-64981.html

[32] Singh K, The Beginner's Guide to Google Wallet. [cited 2015 July]. Avaible from: http://mashable.com/2014/07/14/google-wallet-for-beginners/

[33] United States Securities and Exchange Commision, MasterCard Incorporated. [cited 2015 July]. Avaible from: http://www.sec.gov/Archives/edgar/data/1141391/000114139112000003/ma12312011-10xk.htm

[34] Cozina N, Two new Google Wallet features you don't want to miss. [cited 2015 July]. Avaible from: http://www.cnet.com/how-to/new-google-wallet-features-you-dont-want-to-miss/

[35] M. P., Unaprijeđen Google Wallet za Android. [In Croatian]; [cited 2015 July]. Avaible from: http://www.bug.hr/vijesti/unaprijeden-google-wallet-android/126683.aspx

[36] Google Wallet adds new features. [cited 2015 July]. Avaible from: http://www.pymnts.com/news/2015/google-wallet-adds-new-features/#.Vfk61TYVjIW

[37] Paya C, Coin vs Google Wallet: comparing card aggregation designs. [cited 2015 July]. Avaible from: https://randomoracle.wordpress.com/2014/06/14/coin-vs-google-wallet-comparing-card-aggregation-designs-part-ii/

[38] Geuss M, How Apple Pay and Google Wallet actually work. [cited 2015 August]. Avaible from: http://arstechnica.com/gadgets/2014/10/how-mobile-payments-really-work/

[39] NFC admin, Google Wallet 2.0: Any Credit/Debit Card on an Android. [cited 2015 August]. Avaible from: http://www.nfc.cc/2012/08/03/google-wallet-2-0-any-creditdebit-card-on-an-android/

[40] Wu J, Secure Mobile Money. [cited 2015 August]. Avaible from: http://www.slideshare.net/JamesWu16/secure-qr-code-payment

[41] Griffits R, From ARPANET to World Wide Web [Image on the Internet]. [cited 2015 May]. Avaible from: http://www.let.leidenuniv.nl/history/ivh/chap2.htm

[42] Ekstrom K, E-commerce history: Part 1 – The early years. [Image on the Internet]. [cited 2015 May]. Avaible from: http://christopherekstrom.com/2012/07/16/e-commerce-history-part-1-the-early-years/

[43] Internet service provider. [Image on the Internet]. [cited 2015 May]. Avaible from: https://en.wikipedia.org/wiki/Internet_service_provider

[44] Leff G, Boarding area. [Image on the Internet]. [cited 2015 May]. Avaible from: http://viewfromthewing.boardingarea.com/wp-content/uploads/2009/06/nnc1955credcardb.jpg

[45] Discover Card. [Image on the Internet]. [cited 2015 May]. Avaible from: http://www.myjourneytomillions.com/wp-content/uploads/2010/07/old-discover_card.jpgć

[46] Prasad B, ICICI bank launched contactless credit and debit card. [Image on the Internet]. [cited 2015 June]. Avaible from: http://banking.mercenie.com/business/icici-bank-launched-contactless-credit-debit-card/

[47] O'Rourke J, Revolution at our fingertips. [Image on the Internet]. [cited 2015 June]. Avaible from: http://www.smh.com.au/articles/2003/11/09/1068329417907.html

[48] Biometrics. [Image on the Internet]. [cited 2015 June]. Avaible from: https://upload.wikimedia.org/wikipedia/commons/3/3c/Biometric_system_diagram.png

[49] Contact smart card. [Image on the Internet]. [cited 2015 June]. Avaible from: http://www.plasticpvccard.com/contact-smart-card--1371479.html

[50] Centralized and Decentralized Distributed System. [Image on the Internet]. [cited 2015 June]. Avaible from: http://cffn.ca/img/articles/Centralized-Decentralized-And-Distributed-System.jpg

[51] Electronic money. [Image on the Internet]. [cited 2015 June]. Avaible from: http://emoney.eu.com/fileadmin/emoney/images/tech_slide_EN_thumb.jpg

[52] Electronic money graph [Image on the Internet]. [cited 2015 June]. Avaible from: https://www.ecb.europa.eu/press/pr/date/2013/shared/img/pr130910.en_img000.jpg

[53] Advanced Card System Holdings Limited, Secure Access Module Card. [Image on the Internet]. [cited 2015 June]. Avaible from: http://www.acs.com.hk/en/products/20/acos6-sam-secure-access-module-card/

[54] Digital Era, Encryption with Gnu Privacy Guard (GPG). [Image on the Internet]. [cited 2015 June]. Avaible from: http://digital-era.net/encryption-with-gnu-privacy-guard-gpg/

[55] Fraud losses on French-Issued Cards at French Retailers. [Image on the Internet]. [cited 2015 June]. Avaible from: http://blog.unibulmerchantservices.com/wp-content/uploads/2012/07/Face-to-Face-Fraud-Losses-on-French-Issued-Cards.png

[56] eWallet Payment Account. [Image on the Internet]. [cited 2015 June]. Avaible from: http://www.dixipay.com/ewallet-payment-account/

[57] Edward C, Test Run: Google Wallet's tap-and-pay system is simple. [Image on the Internet]. [cited 2015 August]. Avaible from: http://usatoday30.usatoday.com/tech/columnist/edwardbaig/story/2011-09-21/ed-baig-google-wallet-review/50500628/1

POPIS SLIKA

Slika 2.1. Prikaz početka ARPANET mreže, [41]..... 4

Slika 2.2. Rast uporabe Interneta kroz godine, [42]..... 5

Slika 2.3. TCP/IP Internet karta iz 1986. godine, [43]..... 6

Slika 2.4. Primjer prve Diners Club kreditne kartice, [44]..... 8

Slika 2.5. Primjer Discover Card – a, [45]..... 9

Slika 2.6. Bežična naplata, [46]..... 11

Slika 2.7. Naplata očitanjem otiska prsta, [47]..... 13

Slika 2.8. Dijagram biometrijske naplate, [48]..... 14

Slika 3.1. Presjek pametne kartice, [49]..... 17

Slika 3.2. Razlika između topologije sustava, [50]..... 18

Slika 3.3. Princip rada elektroničkog novca, [51]..... 19

Slika 3.4. Statistika načina naplate do 2012. godine, [52]..... 21

Slika 3.5. Graf prikazuje porast kupovine s elektroničkim novcem, [53]..... 22

Slika 3.6. Prikaz ubrzanog rasta trenda elektroničkog novca, [19]..... 24

Slika 3.7. Izgled SAM kartice, [53]..... 27

Slika 3.8. Primjer enkripcije, [54]..... 28

Slika 3.9. Princip komunikacije prilikom izrade potpisa, [25]..... 30

Slika 3.10. Grafikon koji prikazuje gubitke sa prijevarom na karticama u Francuskoj, [55]..... 32

Slika 4.1. Prikaz sustava elektroničkog novčanika, [56]..... 33

Slika 4.2. SingleTap NFC tehnologija, [57]..... 35

Slika 4.3. Mogućnost praćenja transakcija, [30]..... 37

Slika 4.4. Korištenje PIN – a, [30]..... 38

Slika 4.5. Prikaz prozora za popunjavanje podataka, [32]..... 39

Slika 4.6. Prikaz načina dodavanja novca na račun, [32]..... 40

Slika 4.7. Način aktiviranja i nabavke kupovne kartice, [32]. 40

Slika 4.8. Interakcija kartične transakcije, [33]. 41

Slika 4.9. Postavke za odabir obavijesti upozorenja, [34]. 42

Slika 4.10. Korisnik odabire ponavljajući datum, [34]. 42

Slika 4.11. Prikaz karte obavljenih transakcija, [36]. 43

Slika 4.12. Prikaz arhitekture Google Wallet-a i virtualnih kartica, [37]. 44

Slika 4.13. Stranke uključene u kartični program, [38]..... 46

Slika 4.14. Princip komunikacije prilikom naplate, [39]. 47

Slika 4.15. Prikaz arhitekture Google Wallet platforme (Visio) Izvor:[40] 48

Slika 0.1. Prikaz izgleda anketnog upitnika..... 80

POPIS GRAFIKONA

Grafikon 1. Opredjeljenje prema spolu 51

Grafikon 2. Dobna skupina 51

Grafikon 3. Prikaz statusa ispitanika 52

Grafikon 4. Preferirani način naplate 52

Grafikon 5. Prikaz stope korištenja e - novca 53

Grafikon 6. Pitanje o mišljenju da li e - novac budućnost 53

Grafikon 7. Oblik elektroničkog plaćanja 54

Grafikon 8. Pitanje o definiranju razloga zašto "Ne 54

Grafikon 9. Vrsta elektroničke naplate koja se koristi 55

Grafikon 10. Zadovoljstvo sa uslugom elektroničke naplate 56

Grafikon 11. Korištenje uređaja koji podržava NFC 56

Grafikon 12. Postotak ispitanika koji su čuli za uslugu "Google Wallet" 57

Grafikon 13. Pitanje o zainteresiranosti za Google Wallet uslugu 57

Grafikon 14. Pitanje o razlogu zašto bi ispitanici željeli koristiti uslugu NFC naplate 58

Grafikon 15. Pitanje o razlogu zašto ne bi željeli koristiti uslugu NFC naplate 58

Grafikon 16. Postotak kupnje preko Interneta 59

Grafikon 17. Razlog zašto se ne kupuje preko Interneta 59

Grafikon 18. Razlog kupnje preko Interneta 60

Grafikon 19. Web stranice koje se koriste za kupnju preko Interneta 61

Grafikon 20. Mišljenje o sigurnosti elektroničke naplate 61

Grafikon 21. Iskustva sa sigurnosnim propustima 62

Grafikon 22. Pitanje o elektroničkim transakcijama 63

Grafikon 23. Vlastito mišljenje o razvijenosti elektroničke naplate u RH 63

Grafikon 24. Učestalost korištenja usluga elektroničke naplate 64

Grafikon 25. Zadovoljstvo dostupnošću usluga elektroničkog plaćanja 64

Grafikon 26. Uočene negativnosti ili mane korištenja usluga elektroničke naplate..... 65

PRILOG DIPLOMSKOG RADA

U prilogu diplomskog rada su anketna pitanja. Anketa se sastojala od 28. pitanja,a ona su sljedeća (u zagradama su mogući odgovori):

1. **Vaš spol?** (M/Ž);
2. **U koju dobnu skupinu pripadate?** (18-25, 25-30, 30-40, 40 na više);
3. **Vi ste?** (Student/ica, Zaposlen/a, Nezaposlen/a, Umirovljen/a);
4. **Koji način naplate više preferirate?*** (Gotovina, Kartica, Mpay, Ipay);
5. **Da li ste koristili "Elektronički novac" (E - novac je instrument plaćanja, novčana vrijednost pohranjena na nekom elektroničkom nositelju podataka.)? *** (Da, Ne, Nisam čuo/la za to);
6. **Smatrate li da je elektronički novac budućnost, te da će zamijeniti gotovinu?** (Da - budućnost je samo u e - novcu, Ne - uvijek će postojati gotovina);
7. **Da li koristite neki oblik elektroničkog plaćanja? *** (Da, Ne);
8. **Ako je Vaš odgovor na prošlo pitanje bio "Ne" onda označite razlog zašto.** (Nije me zanimalo, Nije mi potrebno, Sa elektroničkom naplatom mi je ugrožena sigurnost, Nisam imao/la vremena, Nisam upućen/a, Ne volim davati osobne podatke na Internet , Ostalo);
9. **Koju ste vrstu elektroničke naplate koristili?** (PayPal, PayWay, Wave2pay, Apple Pay, Naplata debitnom karticom (npr. maestro), Naplata kreditnom karticom (npr. mastercard), SMS parking, Ostalo);
10. **Da li ste općenito zadovoljni sa uslugom elektroničke naplate?** (Zadovoljan/na sam, Nisam zadovoljan/la);
11. **Ako niste zadovoljni ukratko pojasnite zašto.**
12. **Da li koristite mobilni uređaj koji podržava NFC tehnologiju? *** (Da, Ne);
13. **Da li ste čuli za uslugu elektroničke naplate "Google Wallet"? *** (Da, Ne);

14. **Biste li željeli koristiti mobilni uređaj u svrhu naplate preko NFC - a (npr. Google Wallet)? *** (Da, Ne, Nisam nikad čuo/la za to);

15. **Ukoliko bi željeli koristiti, navedite razlog zašto?** (Jednostavna naplata, Ne moram imati gotovinu uz sebe, Ušteda vremena na blagajni, Volim biti u skladu sa tehnologijom, Imam potpuni pregled povijesti naplate, što s gotovinskom naplatom nemam, Ostalo);

16. **Ukoliko smatrate da naplata preko NFC - a nije za Vas, navedite razlog zašto?** (Nemam osječaj koliko trošim, Nemam povjerenja u elektronsku naplatu, Takva usluga još nije dovoljno sigurnosno razvijena da bih je koristio, Bojim se neovlaštenog korištenja mobilnog uređaja, Navikao/la sam samo na gotovinsku naplatu, Nemam nikakve potrebe za tim, Ostalo);

17. **Da li kupujete ili ste kupovali preko Interneta? *** (Da, Ne);

18. **Ukoliko je Vaš odgovor na prethodno pitanje "Ne", zašto?** (Nemam povjerenja u transakcije preko Interneta, Nisam upoznat/a s tim, Nikad nisam imao potrebe, Nije sigurno, Ostalo);

19. **Koji Vam je primarni razlog zbog kojeg kupujete preko Interneta?** (Jeftinije je, Veći je izbor, Preglednije je, Jednostavnije je, Ostalo);

20. **Koje web stranice za kupovanje preko Interneta koristite?** (eBay, Asos, Amazon, eBid, Craigslist, Ostalo);

21. **Da li smatrate da Vam je elektroničkom naplatom ugrožena sigurnost? *** (Da, Ne);

22. **Da li ste imali iskustva sa sigurnosnim propustom bilo koje vrste pri elektroničkoj naplati?** (Da, Ne);

23. **Ako je odgovor na prošlo pitanje bio "Da", napišite o kakvom se sigurnosnom propustu radi.**

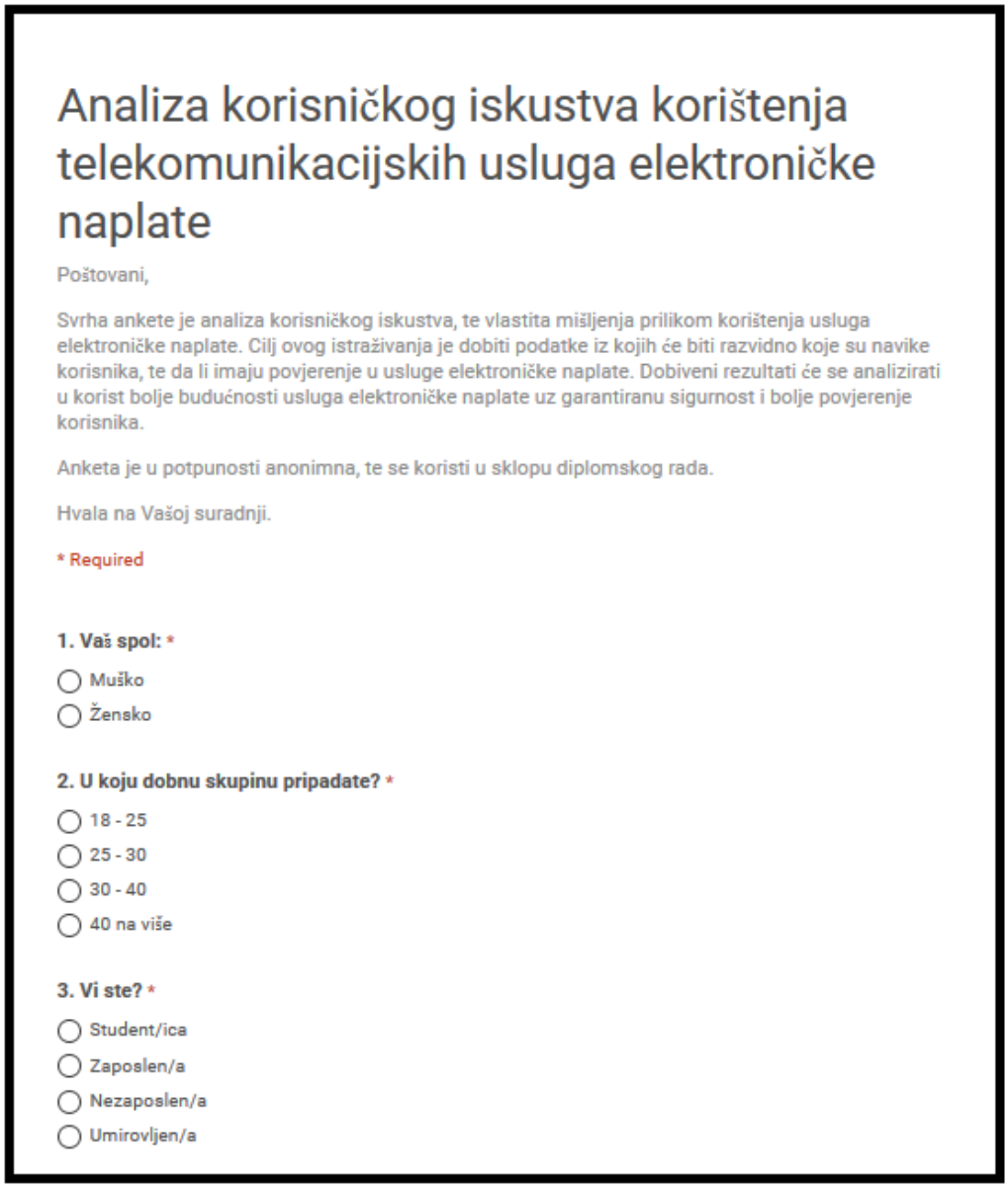
24. **Kod elektroničkih transakcija novca bitno Vam je? *** (Sigurnost, Brzina, Pouzdanost aplikacije, Jednostavnost, Ostalo);

25. **Ocijenite po vlastitom mišljenju trenutnu razvijenost elektroničke naplate u Republici Hrvatskoj. *** (Loša, Dobra, Vrlo dobra, Odlična);

26. **Koliko otprilike često koristite usluge elektroničke naplate?** (Svaki dan, 1 - 2 puta tjedno, Jednom mjesečno, Jednom u par mjeseci, 1 - 2 puta godišnje);

27. **Da li ste zadovoljni dostupnošću usluga elektroničkog plaćanja? (ljestvica: 5 - zadovoljan sam , 1 - nisam zadovoljan) ***

28. **Ukoliko ste uočili neke negativnosti ili mane korištenja usluga elektroničke naplate, o čemu se radilo?** (Blokiranje aplikacije za elektroničku naplatu, Nemogućnost očitavanja NFC taga, Nestanak baterije na uređaju prilikom procesa naplate, Hakerski napad, Ostalo).



Analiza korisničkog iskustva korištenja telekomunikacijskih usluga elektroničke naplate

Poštovani,

Svrha ankete je analiza korisničkog iskustva, te vlastita mišljenja prilikom korištenja usluga elektroničke naplate. Cilj ovog istraživanja je dobiti podatke iz kojih će biti razvidno koje su navike korisnika, te da li imaju povjerenje u usluge elektroničke naplate. Dobiveni rezultati će se analizirati u korist bolje budućnosti usluga elektroničke naplate uz garantiranu sigurnost i bolje povjerenje korisnika.

Anketa je u potpunosti anonimna, te se koristi u sklopu diplomskog rada.

Hvala na Vašoj suradnji.

* Required

1. Vaš spol: *
- Muško
- Žensko

2. U koju dobnu skupinu pripadate? *
- 18 - 25
- 25 - 30
- 30 - 40
- 40 na više

3. Vi ste? *
- Student/ica
- Zaposlen/a
- Nezaposlen/a
- Umirovljen/a

Slika 0.1. Prikaz izgleda anketnog upitnika