Mogućnosti primjene QR kodova u funkciji mobilnog poslovanja

Ćurić, Žarko

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

MOGUĆNOSTI PRIMJENE QR KODOVA U FUNKCIJI MOBILNOG POSLOVANJA

POSSIBILITIES OF THE APPLICATION OF QR CODES IN FUNCTION OF MOBILE BUSINESS

Mentor: doc. dr. sc. Marko Periša

Student: Žarko Ćurić

JMBAG:0135 229 574

Zagreb, rujan 2017.

SAŽETAK

Elektroničko poslovanje je razmjena proizvoda, usluga i novca između kupaca i poslovnih partnera preko informacijsko-komunikacijske mreže koristeći terminalne uređaje. Elektroničko poslovanje nudi mnoge prednosti u odnosu na tradicionalno poslovanje, a razvilo se pojavom interneta i informacijskih sustava. Kratko je opisan poslovni model B2C, budući se on koristi kod mobilnog plaćanja upotrebom QR koda, a opisane su i neke od metoda plaćanja mobilnog elektroničkog poslovanja: kartično poslovanje, mobilno plaćanje pomoću NFC tehnologije, mobilno plaćanje pomoću SMS poruka, mobilno plaćanje pomoću bluetooth tehnologije. Naglasak ovog rada je na primjeni QR kodova u mobilnom plaćanju, pa su se navele opće odrednice o QR kodovima, povijest nastanka, vrste i primjena QR kodova kako bi se dobila cjelokupna slika o toj tehnologiji. Provedena je anketa o korištenju usluga mobilnog elektroničkog poslovanja kako bi se analiziralo korisničko iskustvo ispitanika. Iz ankete se pokušalo saznati zašto ispitanici koriste/ne koriste te usluge, a naglasak je opet bio na QR kodovima, koliko ljudi znaju o njima, da li ih koriste i koliko često. U radu je napravljena analiza trenutnih mogućnosti plaćanja u svrhu mobilnog poslovanja te će se istražiti mogućnosti primjene QR koda u tu svrhu. Na osnovu prikupljenih spoznaja napravljen je prijedlog arhitekture sustava u svrhu učinkovitijeg mobilnog poslovanja primjenom QR koda.

Ključne riječi: elektroničko poslovanje; metode plaćanja mobilnog elektroničkog poslovanja; QR kodovi; analiza korisničkog iskustva

SUMMARY

Electronic business is the exchange of products, services and money between customers and business partners through the information and communication network using terminal devices and offering many advantages over traditional business, and has emerged with the emergence of Internet and information systems. A business model B2C is briefly described, as it is used in mobile payment using QR code and some of the methods of payment for mobile electronic business are described: card business, mobile payment via NFC technology, mobile payment via SMS, mobile payment via bluetooth technology. The focus of this paper was on applying QR codes in mobile payment, and the general guidelines for QR codes, the history of creation, the type and the application of QR codes were provided to obtain a complete picture of this technology. A survey was conducted on the use of mobile electronic business services to analyze user experience of respondents. The survey tried to find out why the respondents used / did not use these services, and the emphasis was again on QR codes, how many people know about them, did they use it and how often. The paper will analyze the current payment options for mobile business and explore the possibilities of applying QR code for that purpose. Based on the collected knowledge, a system architecture proposal will be made for the purpose of more efficient mobile business using QR code.

Keywords: electronic business; payment methods for mobile electronic business; QR codes; user experience analysis

SADRŽAJ

1 UVOD

Razvoj interneta i računala potaknuo je i nastanak usluge elektroničkog poslovanja. 1990-tih počinju se obavljati prve novčane transakcije na daljinu bez fizičkog kontakta preko terminalnih uređaja i telekomunikacijske mreže. U početku je to bila jednostavna usluga, te su se kasnije počele dodavati i brojne nove usluge: jednostavno pretraživanje ponude po internet stranici, dogovoranje detalja oko kupnje i isporuke, naručivanja proizvoda i usluga ili samog elektroničkog plaćanja (putem kartice, odjednom ili na više rata, preko raznih internet servisa - „*Paypal*“...). Elektroničko poslovanje brzo se raširilo među tvrtkama koje su prepoznale veliki potencijal i mnogo pozitivnih stvari koje ono nudi. Elektroničko poslovanje je u svom razvoju doživjelo i jednu krizu, ali se vrlo brzo izvuklo iz nje. Kako je najvažniji segment kod elektroničkog poslovanja naplata, odnosno plaćanje, razvijene su i različite metode plaćanja, a spomenut će se neke od njih: kartično poslovanje, mobilno plaćanje pomoću NFC tehnologije, mobilno plaćanje pomoću SMS poruka, mobilno plaćanje pomoću bluetooth tehnologije. Plaćanje pomoću QR kodova jedna je od relativno novih metoda plaćanja koja je opisana u ovom diplomskom radu. Kroz općeniti opis, povijest nastanka, vrste i primjenu QR kodova pokušano je bolje objasniti i približiti ovu tehnologiju širokoj populaciji. Svrha diplomskog rada je objasniti pojam „elektroničkog poslovanja“, nabrojati i objasniti metode plaćanja mobilnog elektroničkog poslovnja i pokazati primjenu u praksi. Cilj diplomskog rada je napraviti analizu trenutnih mogućnosti plaćanja u svrhu mobilnog poslovanja, te istražiti mogućnosti primjene QR koda u tu svrhu, ali i na osnovu prikupljenih spoznaja napraviti prijedlog arhitekture sustava u svrhu učinkovitijeg mobilnog poslovanja primjenom QR koda.

Naslov diplomskog rada je: **Mogućnosti primjene QR kodova u funkciji mobilnog poslovanja.** Rad je podijeljen u sedam cjelina:

1. Uvod
2. Definicija i opće značajke elektroničkog poslovanja
3. Metode plaćanja mobilnog elektroničkog poslovanja
4. QR kodovi

5. Analiza korisničkog iskustva pri korištenju usluga mobilnog elektroničkog poslovanja
6. Prijedlog arhitekture za mobilno plaćanje pomoću QR koda
7. Zaključak

U drugom poglavlju navedena je definicija elektroničkog poslovanja, karakteristike, elementi, prednosti i nedostaci te klasifikacija elektroničkog poslovanja.

U trećem poglavlju nabrojane su i objašnjene metode plaćanja mobilnog elektroničkog poslovanja: kartično poslovanje, mobilno plaćanje pomoću NFC tehnologije (Google Wallet), mobilno plaćanje pomoću SMS poruka, mobilno plaćanje pomoću bluetooth tehnologije (TWINT).

U četvrtom poglavlju detaljno su opisani QR kodovi, njihov povijesni razvoj, vrste i primjena QR kodova.

U petom poglavlju prikazana je analiza dobivenih rezultata iz anketnog upitnika koji sadrži pitanja o korisničkom iskustvu prilikom korištenja usluga mobilnog elektroničkog poslovanja.

U šestom poglavlju prikazan je i objašnjen prijedlog arhitekture za mobilno plaćanje pomoću QR koda.

2 DEFINICIJA I OPĆE ZNAČAJKE ELEKTRONIČKOG POSLOVANJA

Postoji nekoliko definicija elektroničkog poslovanja. Andrew Bartel, potpredsjednik i voditelj istraživanja kompanije Giga Information Group, kaže da je elektroničko poslovanje „Razmjena proizvoda i usluga između kupaca, poslovnih partnera i prodavatelja. Primjerice, dobavljač integrira s proizvođačem, kupci s prodavačima, a otpremnici (špediteri) s distributerima. Elektroničko poslovanje čine svi ti elementi, ali i operacije što se obavljaju unutar samo tvrtke.“ E-poslovanje (*e-Business*) nastalo je rastućom primjenom informacijske tehnologije u poslovanju, i u skladu s tim sve poslovne aktivnosti izvršavaju se elektroničkim putem. U odnosu na tradicionalno poslovanje donosi veću interaktivnost, bolju povezanost i fleksibilnost, te je jeftinije i brže [1].

Elektroničko poslovanje se pojavilo i zahvaljujući pojavi i razvoju interneta te informacijskih sustava. Internet predstavlja računalnu mrežu sastavljenu od više stotina tisuća manjih mreža koje su međusobno povezane i spajaju različite uređaje iz cijelog svijeta. Uređaji šalju različite informacije korištenjem protokola za kontrolu prijenosa podataka, od kojih je najrašireniji *Transmission Control Protocol/Internet Protocol* (TCP/IP).

Što se tiče informacijskih sustava, oni su obično podskup nekog šireg i većeg organizacijskog sustava. Osnovna uloga im je povezati elemente neke organizacije, omogućiti međusobnu komunikaciju između tih istih elemenata, a nekakav osnovni cilj je dostaviti informaciju na pravo mjesto u pravo vrijeme uz minimalne troškove. Svaki informacijski sustav sadrži sljedeće elemente: *hardver, softer, lifeware, orgware, netware i dataware*. *Hardver* ili sklopovlje predstavlja fizičku komponentu sustava, opremu i ostale dijelove koji čine materijalnu osnovicu računala, dok bi *softver* predstavljao nematerijalni dio informacijskog sustava, dakle nekakav skup programa koji upravljaju ili se izvode na računalu. *Orgware* predstavlja organizacijski dio sustava, a sastoji se od postupaka, metoda, procedura i načina povezivanja ostalih komponenti sustava. *Lifeware* predstavlja ljudsku komponentu u sustavu (operateri, projektanti, serviseri..). *Netware* predstavlja komunikacijsko povezivanje elemenata i dijelova sustava u cjelini, dok *dataware* predstavlja organizaciju baze podataka i informacijskih resursa [2].

2.1 Karakteristike elektroničkog poslovanja

E-poslovanje kao takvo pokušava pojednostaviti sve procese unutar tvrtke pa je tako i kod razvoja proizvoda, gdje doprinosi razvoju proizvoda unutar kraćeg vremenskog razdoblja zadržavajući istu kvalitetu proizvoda smanjujući ujedno i troškove. Što se tiče zajedničkog planiranja, predviđanja i nadopunjavanja, kod elektroničkog poslovanja partneri rade zajedničku prognozu ili plan u kojem proizvođači, distributeri i trgovci prikupljaju tržišne informacije o proizvodima i dijele ih u stvarnom vremenu putem mreže. Kod nabave, povećanja sposobnosti kupnje i redoslijeda upravljanja tvrtke koriste integrirane elektroničke procese i ostale online resurse. Pojednostavljenjem procesa nabave, nadzorom zaliha i promatranjem učinkovitosti kupnje tvrtke postižu uštede te ostvaruju bolju kvalitetu usluge za krajnjeg korisnika. Još jedna karakteristika elektroničkog poslovanja je izvrsno rukovanje i logistika, koje se očituje u dobrom planiranju, implementaciji i kontroliranju pohrane dobara, usluga ili informacija iz izvorišne točke do krajnjeg korisnika, odnosno točke konzumacije. To je omogućeno zajedničkim i usklađenim radom transporta, skladištenja, distribucije, kupnje i nabave.

2.2 Elementi elektroničkog poslovanja

Prvi, a možda i najvažniji element elektroničkog poslovanja je upravljanje odnosnom s kupcima (*Customer Relationship Managment – CRM*). To je integrirana prodajna, marketinška i uslužna strategija koja zahtijeva koordiniranu akciju od stranu svih odjela organizacije [3]. CRM ima tri faze: stjecanje novih korisnika, povećanje profitabilnosti postojećih korisnika i zadržavanje profitabilnih kupaca. Neki od najvažnijih ciljeva CRM-a su:

- brže dohvaćanje i protok informacija, sprečavanje gubitka informacija,
- povećanje zadovoljstva i razine usluge kod kupaca,
- automatizacija i ubrzanje poslovnih procesa prodaje i marketinga,
- produženje odanosti kupaca,
- lakše prepoznavanje dobrih poslovnih prilika i potencijala,
- segmentacija kupaca na temelju ekonomskih, socijalnih i demografskih podataka,
- bolje planiranje poslovnih aktivnosti,

- lakše praćenje rada zaposlenika i njihovih rezultata prodaje [3].

Drugi element elektroničkog poslovanja je planiranje resursa poduzeća (*Enterprise Resource Planning systems* – ERP). Planiranje resursa poduzeća predstavljaju poslovni informacijski sustavi koji povezuju i automatiziraju velik broj poslovnih radnji povezanih s operacijama ili dijelovima proizvodnje tvrtke. Planiranje uključuje proizvodnju, logistiku, distribuciju, zalihe, otpremu itd., a sastoji se od četiri poslovna procesa:

- proizvodnja, odnosno planiranje resursa proizvodnje i procesa izvršavanja,
- postupak nabave ili kupovanje proizvoda,
- prodaja proizvoda i usluga,
- određivanje cijene, plaćanje računa i prikupljanje, odnosno proces financijskog upravljanja i izvještavanja [4].

Treći element elektroničkog poslovanja je upravljanje lancem opskrbe (*Supply Chain Managment*) koji predstavlja mrežu objekata koja ima mogućnost distribucije koje obavljaju funkcije nabave materijala, pretvorbe u posredne i gotove proizvode, te distribuciju gotovih proizvoda potrošačima. Tri glavna elementa lanca opskrbe su: nabava, proizvodnja i distribucija. Četvrti element je upravljanje znanjem čime se analizira dostupna i potrebna imovina znanja (obuhvaća informacije i iskustvo). Upravljanje znanjem se odnosi na znanje tvrtke o tržištu, proizvodima, procesima, tehnologijama koje tvrtka posjeduje ili treba posjedovati. Peti element elektroničkog poslovanja je e-tržište koje predstavlja elektroničko mjesto za kupce i prodavače na kojemu se mogu pregledati svi proizvodi i usluge, koristi internet za povezivanje većeg broja kupaca i pomoću njega prodavači lakše komuniciraju i upravljaju poslovanjem [5].

2.3 Prednosti i nedostaci elektroničkog poslovanja

E-poslovanje prestavlja široku paletu poslovnih i tehnoloških rješenja koja omogućavaju upravljanje različitim poslovnim procesima kao što su računovodstvo, pohrana podataka, proizvodni procesi, ljudski resursi. Upravljanje poslovanjem može se poboljšati upravo korištenjem alata za e-poslovanje. Tvrtke uz pomoć elektroničkih sustava, odnosno korištenjem elektroničkog poslovanja mogu povezati svoje

poslovne procese, stvaranje i protok podataka i dokumenata u jedinstvenu poslovnu cjelinu uključujući nabavljače i partnere, te omogućiti kvalitetnije zadovoljavanje očekivanja i potrebe korisnika. E-poslovanje predstavlja ne samo način povećanja prodaje, ulazak na novo tržište ili smanjenje troškova poslovanja, nego i povećanje djelotvornosti i učinkovitosti cijele tvrtke poboljšanjem procesa unutarnjeg upravljanja. Prednosti e-poslovanja u tvrtkama:

- mogućnosti smanjenja troškova poslovanja kroz automatizaciju poslovanja i automatizaciju podrške,
- povećanje prodaje korištenjem online transakcija, davanje kvalitetnijih informacija o proizvodima/uslugama, omogućena dostupnost većem broju korisnika,
- mogućnost pristupa novim tržištima (inozemstvo) korištenjem web stranica, olakšanje prilagodbe proizvoda korisnicima,
- mogućnost pristupa proizvodima i uslugama 24/7 korištenjem online shopova i kataloga,
- preciznije informacije i poboljšanje kvalitete podrške korisnicima (pregled narudžbi, post prodajne aktivnosti, online računi),
- poboljšanje efikasnosti lanca nabave (uvid u dostupnost, uvid u status/lokaciju, upravljanje proizvodnjom, elektronička nabava, uštede na skladištu),
- mogućnost uvida u stanje poslovanja u realnom vremenu,
- poboljšanje radnih uvjeta zaposlenika (rad od kuće, klizno radno vrijeme),
- mogućnost preciznog pronalaženja ciljanih korisnika [6].

U prvom redu nedostaci elektroničkog poslovanja odnose se na sigurnost i prijevare. U stvarnosti i kupci i prodavači moraju strahovati od određenog rizika od prijevare. Prodavači riskiraju gubitak ili krađu korisničkih podataka kreditnih kartica, dok kupci se kupci suočavaju s rizikom od nepoznatih stranica, te bi trebali proučavati statuse tih stranica i koristiti što sigurnije oblike plaćanja. Virusi, *spam* poruke i različiti zlonamjerni *softveri* također ometaju cijeli proces e-poslovanja, te se korisnici moraju zaštititi prvenstveno na samom uređaju preko koje posluju.

Još jedan nedostatak kod e-poslovanja je nemogućnost fizičkog dodira s proizvodom, koji se očituje najviše kod odjeće i svježih namirnica. Također, prekidi poslovanja uzrokovani nekakvim vanjskim čimbenicima (nestanak struje, greška

poslužitelja) mogu dovesti do gubitka povjerenja kupaca. Kao rezultat tih problema postoji nedostatak povjerenja prema e-poslovanju, međutim ono je sve manje budući da se e-poslovanje proširilo i da je sve zastupljenije na potrošačkim tržištima [6].

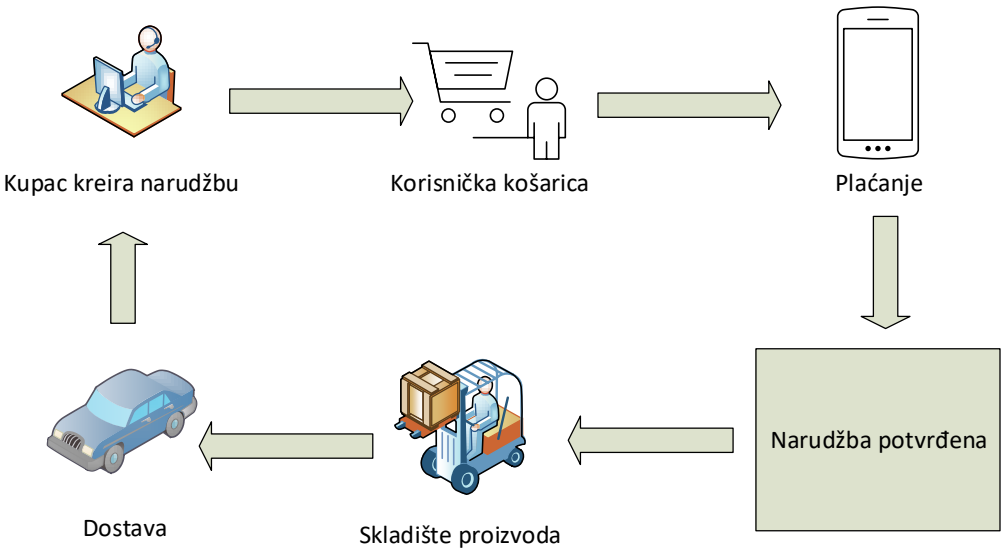
2.4 Klasifikacija elektroničkog poslovanja

U elektroničkom poslovanju poslovanje se može obavljati između tri strane: vlade (*Government*), kompanije (*Business*) i klijenta (*Consumer*). Prema ranije navedenim stranama komunikacija se može odvijati između:

- kompanije i krajnjih korisnika
    - *Business to Business* (B2B),
    - *Business to Consumer* (B2C),
    - *Consumer to Business* (C2B),
    - *Consumer to Consumer* (C2C),
    - *Business to Employee* (B2E),
    - *Employee to Business* (E2B).
- unutar elektronske vlade
    - *Business to Government* (B2G),
    - *Government to Business* (G2B),
    - *Government to Government* (G2G),
    - *Government to Consumer* (G2C).
- i između više strana, odnosno višestruke transakcije (B2B2C, C2B2C, P2P...) [1].

Pošto će se u radu kasnije opisati princip mobilnog plaćanja pomoću primjene QR koda, detaljnije će se opisati *Business to Consumer* (B2C) model budući da predstavlja upravo taj način komunikacije. B2C komunikacija predstavlja direktnu poslovnu suradnju između tvrtke i klijenta, gdje klijent bira između više proizvoda, usluga ili informacija te olaća određenu naknadu za kupovinu istih. Prednosti su mnogobrojne: ušteda vremena, nude mnogo veći izbor i zahtijevaju manje vremena za pretraživanje tržišta i konkurencije, velika je ponuda i potražnja što automatski snižava cijene nego u klasičnim trgovinama.

Princip rada B2C modela prikazuje slika 2.1. Na slici je prikazan korisnik koji kreira narudžbu preko internet stranice. U košaricu se ubacuju proizvodi koje kupac odabire i koji su trenutno dostupni na skladištu. Nakon odabira proizvoda, slijedi plaćanje koje može biti izvedeno na razne načine (karticom, paypal računom, QR kodom...). Kada je plaćanje gotovo, narudžba je potvrđena i šalje se u skladište, gdje se proizvod uzima i dalje dostavlja na kućnu adresu kupca.



Slika 2.1. B2C poslovni model

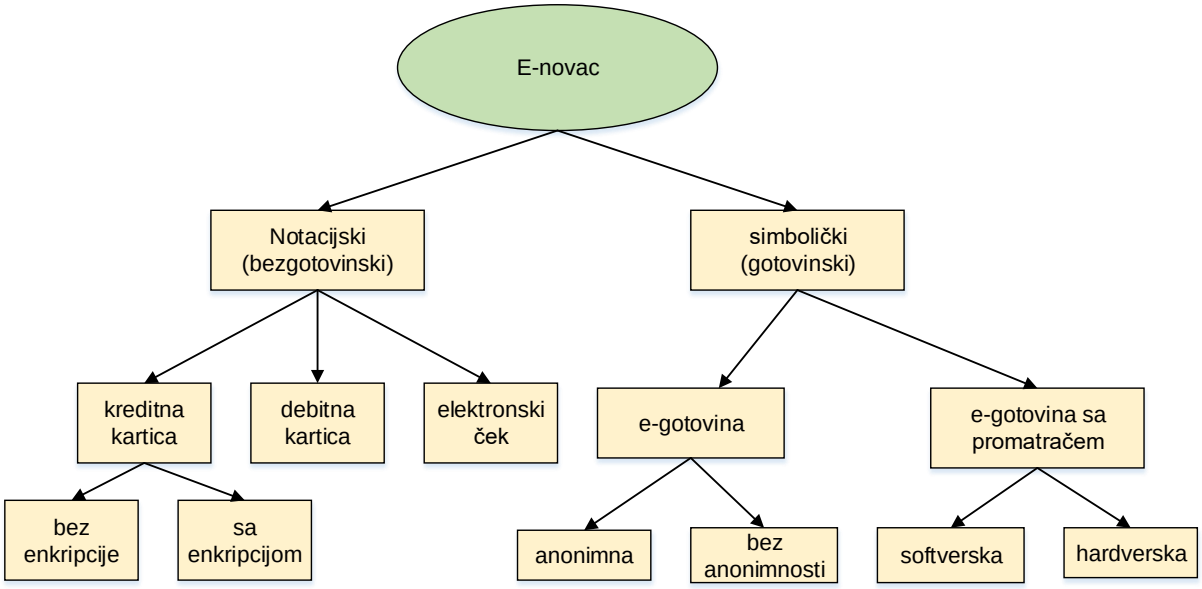
Kako je upotreba QR kodova jedna od metoda plaćanja kod elektroničkog poslovanja te ujedno i jedna od tema ovog diplomskog rada, kasnije u nastavku rada će se detaljnije objasniti nastanak, vrste, funkcioniranje i princip rada QR kodova, te njihova primjena u realnim situacijama.

3 METODE PLAĆANJA MOBILNOG ELEKTRONIČKOG POSLOVANJA

Elektroničko plaćanje je zaseban dio elektroničkog poslovanja koje se sastoji od niza međukoraka na kraju kojih je plaćanje obavljeno. U postupku elektroničkog plaćanja postoje tri vrste sudionika:

- osoba koja plaća uslugu, proizvod elektroničkim novcem (kupac)
- osoba koja je plaćena elektroničkim novcem u zamjenu za uslugu, proizvod (trgovac)
- izdavač elektroničkih novčanica (banka)

Vrste plaćanja mogu se podijeliti na dvije skupine: notacijsko ili bezgotovinsko i simboličko ili gotovinsko kao što je prikazano na slici 3.1.



Slika 3.1. Elektroničke vrste plaćanja, [7]

Razlika između ovih sustava je u načinu na koji i vremenu kada novac mijenja vlasnika. Notacijski sustav koristi dokument (nalog, ček, karticu) koji sam nema vrijednost, već je on određena potvrda banci gdje je novac pohranjen. Kada se banci predstavi potvrda, ona prebacuje novac s računa kupca na račun trgovca. Simbolički sustav se temelji na simbolu (novčanica ili kovanica) koji nosi u sebi vrijednost.

Kako se elektroničko poslovanje proširilo internetom, razvile su se i različite metode plaćanja elektroničkog poslovanja, pa tako postoji plaćanje karticom,

mobilnim uređajem, elektroničkim novcem, elektroničkom lisnicom, pomoću internet bankarstva, preko internet servisa (paypal) itd. U nastavku će se objasniti neke od metoda [7].

3.1 Kartično poslovanje

Kreditno kartično poslovanje je bezgotovinsko poslovanje i zapravo sredstvo kratkoročnog kreditiranja gdje je kreditna kartica glavni instrument. Izdavatelj kartice je ujedno i vlasnik, a korisnik ima pravo upotrebe kartice (raspolaže računom 24/7, dostupnost gotovine u svakom trenutku putem bankomata, veća sigurnost raspolaganja novcem). Korisnik može plaćati kontaktno u stvarnom dućanu, fizički provlačeći karticu ili beskontaktno prislanjajući karticu uz platni uređaj.

Prednosti zbog kojih poslodavci prihvaćaju karticu kao platno sredstvo su: povećani promet uslijed velikog broja korisnika i njihovim povećanim korištenjem kartica kao platnog sredstva, smanjeno poslovanje sa gotovinom (manji troškovi, smanjenje rizika), mogućnost prodaje na kredit. Osnovna podjela kartica je prema izdavatelju i roku naplate. Prema izdavatelju kartice se dijele na bankovne (MasterCard i Visa kartice) i nebankovne (American Express, Diners, kartice trgovačkih kuća), dok se prema roku naplate dijele na debitne kartice (Maestro kartice s PIN-om), kartice s odgodom plaćanja i kreditne kartice.

Karakteristike debitnih kartica su:

- trenutna naplata s računa,
- manja vrijednost s transakcije,
- veći broj korisnika kartice,
- kartica je vezana uz tekući račun,
- sigurnost – autorizacija, najčešće PIN-om,
- viši stupanj tehnologije (obavezan EFT POS uređaj ili bankomat),
- niži postotak provizije [8].

Karakteristike kartica s odgodom plaćanja i kreditnih kartica su:

- odgoda plaćanja i obično veće vrijednosti transakcija,
- manji broj korisnika kartice,

- limit potrošnje kartice ovisno o platežnoj moći korisnika,
- sigurnost – potpis, postavljanje limita,
- niži stupanj tehnologije (imprinter),
- veći broj mjesta prihvata, veća provizija.

Postupka plaćanja na prodajnom mjestu, ukoliko se radi o „klasičnom“ kontaktnom plaćanju, može se izvršiti na dva načina: pomoću EFT POS terminala i pomoću imprintera.

EFT POS terminal se koristi za debitne i kartice s odgodom plaćanja ili kreditne kartice. Debitnu karticu prodavač provlači kroz EFT POS uređaj i upisuje iznos te nakon toga daje korisniku PIN PAD uređaj u koji korisnik upisuje svoj PIN, čime potvrđuje svoj identitet. Ukoliko je sve ispravno uneseno, i kartica je u redu, stići će odobrenje transakcije. Ukoliko se radi o kartici s odgodom plaćanja ili kreditnoj kartici, postupak je malo drugačiji. Prodavač također provlači karticu kroz EFT POS uređaj i upisuje iznos nakon čega izlazi listić koji korisnik potpisuje i na taj način potvrđuje transakciju. Dakle umjesto unosa PIN-a korisnik se identificira potpisom, kojeg bi prodavač trebao prekontrolirati uspoređujući ga sa potpisom na poleđini kartice. Ukoliko nema EFT POS uređaja, plaćanje se vrši uz pomoć imprintera. Uz imprinter se koriste isključivo kartice s odgodom plaćanja i kreditne kartice. Imprinter se danas više gotovo i ne koristi pa neće biti detaljno opisan [8].

Beskontaktno plaćanje pojavilo se u 21. stoljeću gdje je doživjelo i svoj veliki rast i primjenu. Beskontaktno plaćanje podrazumijeva način plaćanja kod kojeg kartica ne napušta ruku vlasnika (korisnika), a transakcije do određenog iznosa nije potrebno autorizirati PIN-om ili potpisom. Beskontaktno plaćanje obično se rabi za manje novčane transakcije (do 100 kn po transakciji, odnosno 1000 kn dnevno). Da bi se plaćanje izvršilo dovoljno je karticu prisloniti uz čitač kartice, odnosno POS uređaj. Čitači kartica za beskontaktno plaćanje lako se ugrađuju pa ih zbog toga koriste razni dućani, restorani, benzinske crpke, kiosci, šalteri na kolodvorima itd. Beskontaktno plaćanje danas u svijetu omogućuju *Erste Card Club*, OTP banka, PBZ *Card* i *Raiffeisen* banka [8].

U beskontaktne kartice ugrađeni su računalni čipovi i antene koje omogućavaju da se kartica bežično poveže sa čitačem kartice. Približavanjem kartice čitaču na samo par centimetara, šalju se pojedinosti o plaćanju (vrijeme, iznos, detalji o

korisniku, detalji o prodavaču) prema maestro, visa ili nekoj drugoj kartičnoj mreži. Sama transakcija traje svega par sekundi, a nakon plaćanja korisnik prima potvrdu o izvršenoj uplati te mu se ispisuje POS *slip*[1]. Kod beskontaktnog plaćanja nije potreban potpis ili autorizacija PIN-om upravo iz razloga što bezgotovinske transakcije moraju biti jednostavne i praktične. Prednosti beskontaktnog načina plaćanja su mnoge:

- zamjenjuje gotovinu te na taj način smanjuje manipulaciju i troškove pohranjivanja gotovine,
- transakcije se odvijaju brzo, idealno za mjesta gdje se vrši veliki broj malih transakcija (stadioni, kiosci, dućani, restorani brze hrane..),
- pružatelj ovakve usluge dugoročno ima manje troškove i dobiva na konkurentskoj prednosti,
- povećana sigurnost kod plaćanja (jedna kupnja se ne može naplatiti više puta zbog sigurnosnog koda koji sprječava dupliranje računa za istu transakciju, čak i ukoliko se kartica prinosi čitaču više puta),
- zbog brzine transakcije onemogućuje se neovlašteno pristupanje korisničkim podacima,
- korisnik kontrolira transakcije jer karticu ne ustupa nikome, i ne postoji mogućnost slučajnog plaćanja budući da kartica mora biti prislonjena uz čitač,
- korisnik također može odrediti dnevni limit beskontaktnih transakcija i na taj način se zaštititi u slučaju krađe,
- ukoliko prodajno mjesto ne podržava beskontaktni način plaćanja, korisnik karticu može koristiti na tradicionalan način (autorizacija PIN-om ili potpisom).

Beskontaktna tehnologija plaćanja predstavlja razvoj elektroničkog poslovanja, te ju koristi sve veći broj korisnika prepoznavajući brzinu, sigurnost i praktičnost ove tehnologije. Prema nekim podacima korištenje beskontaktnog plaćanja povećala se 10% u 2014. godini, na 32% u 2015., pa sve do 40% u 2016. godini. Iz ovoga se da zaključiti da će taj trend svakako rasti i da će ga ljudi sve više prihvaćati [9].

[1] POS *slip* - papirnata potvrda koju korisniku kartice u procesu kupnje karticom izdaje POS uređaj ili bankomat kod podizanja gotovine, a služi kao potvrda uspješno obavljene transakcije.

3.2 Mobilno plaćanje pomoću NFC tehnologije

NFC[2] je bežična tehnologija kojom se prenose podaci na kratkim udaljenostima (do nekoliko centimetara). NFC koristi induktivno uparene uređaje koji rade na frekvenciji 13.56 MHz uz protok podataka od 424 kbps. NFC je zamišljen za slanje malih količina podataka (broj transakcije, broj kartice) pa mu stoga i nije potrebna veća brzina od ove. Rad NFC-a se zasniva na principu magnetske indukcije koja se stvara između dvije antene uređaja. Kroz stvoreno inducirano polje šalju se električni impulsi, odnosno podaci. Postoje dva tipa uređaja koji se koriste, a to su prijamnik i predajnik. Prijamnik je pasivni, dakle ne treba mu izvor napajanja, dok ga predajnik mora imati. Zbog toga što im ne treba izvor napajanja, prijamnici mogu biti izvedeni kao naljepnice ili tanki slojevi plastike zbog čega mogu imati vrlo rasprostranjenu primjenu [10].

Postoje tri vrste uređaja koji mogu učestvovati u prijenosu podataka putem NFC tehnologije:

- NFC čitač koji se koristi kao inicijator u NFC komunikaciji,
- Mobilni uređaj može se ponašati kao aktivan i pasivan uređaj, zavisno od potrebe aplikacije u kojoj se koristi,
- NFC *tag* koji predstavlja pasivan uređaj koji može komunicirati sa aktivnim uređajem.

Postoji također i tri načina funkcioniranja između NFC uređaja, a to su:

- *Peer-to-peer* način funkcioniranja predstavlja način komunikacije gdje dva mobilna uređaja komuniciraju preko NFC-a, razmjenjujući podatke na način da jedan uređaj inicira komunikaciju dok drugi odgovara na zahtjev,
- *Read/Write* način rada funkcionira na način da mobilni uređaj sa NFC-om inicira komunikaciju sa *tag*-om, odnosno može pročitati podatke sa *tag*-a ili upisati nove informacije u *tag*,
- NFC *Card* je način koji omogućava mobilnim uređajima sa NFC tehnologijom da se ponašaju kao standardne *smart* kartice, iniciator komunikacije u ovom slučaju je NFC čitač koji ispoljava magnetno polje, te kada se mobilni uređaj

[2] NFC - *Near Field Communication*, odnosno bežična komunikacija na malim udaljenostima.

približi čitaču, mobilni uređaj reagira kao pasivan uređaj i odgovara na zahtjev čitača [10].

Za mobilno plaćanje koristi se postojeća financijska i komunikacijska infrastruktura. Mobilni uređaji sa NFC tehnologijom danas se sve više koriste u plaćanju. Najčešće korisnici imaju instalirane aplikacije uz pomoć koji jednostavnije obavljaju cijeli proces plaćanja. Aplikacija povezuje NFC tehnologiju implementiranu u uređaju sa kreditnim i debitnim karticama koje korisnik posjeduje te prilikom plaćanja skida određeni iznos sa računa. Aplikacija i informacije su šifrirane, te ih se ne može lako ukrasti niti iskoristiti u razne prijevare, međutim najveći sigurnosni aspekt NFC-a je domet tehnologije. Domet je svega par centimetara pa bi svako presretanje podataka bilo preočito za korisnika koji bi odmah mogao reagirati na to.

Proces plaćanja putem mobilnog uređaja koji posjeduje NFC tehnologiju ima nekoliko koraka:

1. Kupac prinosi svoj mobilni uređaj prema čitaču i time šalje zahtjev za naplatom. Taj zahtjev se dalje prosljeđuje PSP-u (*Payment System Provider*) sa iznosom koji se plaća.
2. PSP provjerava stanje računa kupca i vrši se verifikacija zahtjeva.
3. PSP šalje mobilnom uređaju kupca zahtjev za potvrdu kupovine, na koji kupac odgovara potvrdom kupovine.
4. Nakon uspješne potvrde, PSP vrši pozadinsku obradu i ažuriranje računa.
5. PSP šalje potvrdu o kupovini kupcu i prodavaču.

Najčešće korištene mobilne aplikacije odnosno sustavi plaćanja putem NFC-a su *Google Wallet*, *Wave2Pay,* ISIS. Neki od njih se jos i danas koriste, a neki su jednostavno ugašeni zbog premalog interesa korisnika [11].

3.2.1 Google Wallet

Google Wallet je aplikacija, odnosno sustav naplaćivanja pomoću mobilnih uređaja. Razvijen od strane *Google*-a omogućava korisnicima da svoje kreditne, debitne i prepaid kartice pohrane na jedan uređaj koji će im biti uvijek pri ruci. *Google Wallet* koristi NFC tehnologiju u svrhu naplate, odnosno prijenosa informacija o korisniku, iznosu plaćanja i kartici prema naplatnom terminalu. *Google Wallet*

omogućuje brzu i sigurnu naplatu za korisnika koji u tom trenutku ne može ili ne želi platiti gotovinom, a posjeduje određena sredstva na svom bankovnom računu. Osim pohrane kreditnih i debitnih kartica, *Google Wallet* omogućava korištenje poklon kartica te iskorištavanje prodajnih promocija uz korištenje mobilnih uređaja sa instaliranom aplikacijom.

3.2.2 Sigurnosni aspekti Google Wallet-a

Što se tiče sigurnosti sustava, on je na visokom nivou i pruža nekoliko vrsta zaštite:

- mogućnost zaključavanja: stavljanje 4-znamenkastog PIN-a prilikom ulaska u aplikaciju da bi se zaštitile informacije o karticama od neovlaštenog pristupa ili „*cyber*“ kriminalaca,
- daljinsko upravljanje: u slučaju gubitka ili krađe mobilnog uređaja *Google Wallet* pruža mogućnost udaljenog onesposobljavanja ili blokiranja računa, odnosno pojedine kartice će raditi, ali usluga kupnje preko *Google Wallet*-a neće biti omogućena,
- enkripcija: kreditne i debitne kartice pohranjene u *Google Wallet*-u su kriptirane na *Google*-ovim sigurnim serverima. Kada korisnik plaća nešto, prvo *Google* plaća trgovca, a zatim obrađuje transakciju s korisnikovom karticom kojom je platio,
- skriveni brojevi računa: aplikacija skriva brojeve računa kartice s kojom se platilo, kada se kartica pojavi na ekranu korisnikovog mobilnog uređaja u trgovini, brojevi nisu vidljivi, već su na mreži vidljive samo 4 zadnje znamenke tijekom kupnje [12].

Google Wallet pojavio se 2011. godine te je u suradnji sa *MasterCard*-om predstavio ovaj način plaćanja. Mobilni uređaj morao je posjedovati NFC tehnologiju da bi mobilno plaćanje bilo moguće. *Google Wallet* pohranjuje informacije korisničkih kreditnih kartica u šifriranom obliku na računalnom čipu mobilnog uređaja zvanog „*Secure Element*“. Čip je odvojen od memorije mobilnog uređaja i može mu se pristupiti isključivo preko programa sa sigurnosnim elementima, na ovaj način štite se

informacije korisničkih kartica. Da bi se spriječilo neovlašteno ili slučajno plaćanje NFC čip je deaktiviran dok je ekran mobilnog uređaja isključen [13].

Da bi korisnike zaštitio od neovlaštenog korištenja *Google* je postavio zaštitu prilikom ulaska u aplikaciju. Potrebno je upisati 4-znamenkasti PIN nakon kojega je omogućeno slanje, podizanje i kupovina pomoću *Google Wallet* aplikacije i mobilnog uređaja. Kako izgleda korištenje PIN-a prikazano je na slici 3.2.

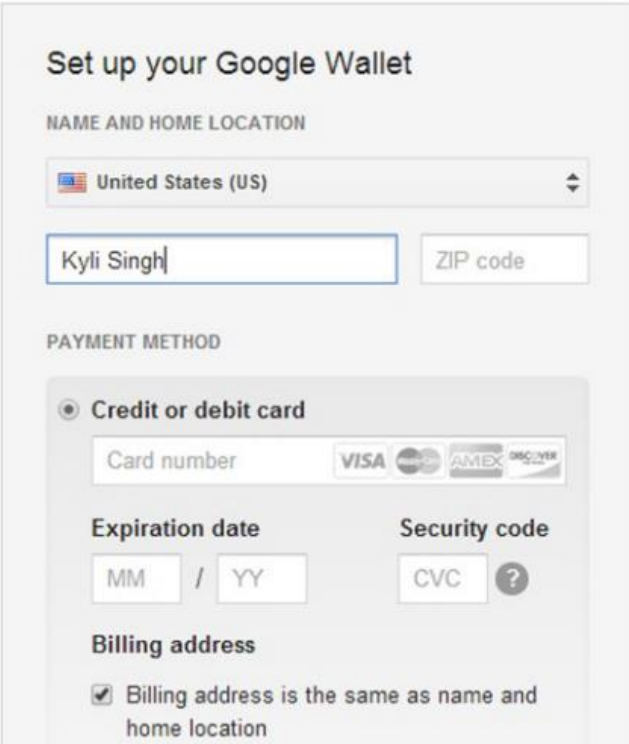
Slika 3.2. Korištenje PIN-a, [14]

Google Wallet može raditi samo na uređajima koji podržavaju sigurnosni čip (*Secure Element).* Sigurnosni čip sadrži informacije o naplati koje su odvojene od glavnog hardvera i procesora, a informacije o naplati su ujedno i kriptirane. Kriptiranje podataka omogućuje da oni ne mogu biti pročitani čak niti za vrijeme transakcije. NFC djeluje na svega par centimetara udaljenosti pa je svako presretanje komunikacije između mobilnog i naplatnog uređaja i više nego očita za korisnika pa je i to jedan veliki sigurnosni aspekt koji ide u prilog ovoj tehnologiji [14].

3.2.3 Instalacija i mogućnosti Google Wallet aplikacije

Da bi mogao koristiti aplikaciju korisnik mora imati otvoren *Google* račun, te ukoliko ga nema mora ga napraviti. Prilikom izrade računa za *Google Wallet*

aplikaciju potrebno je upisati osnovne osobne podatke te podatke o kreditnoj kartici kao što je prikazano na slici 3.3 [16].



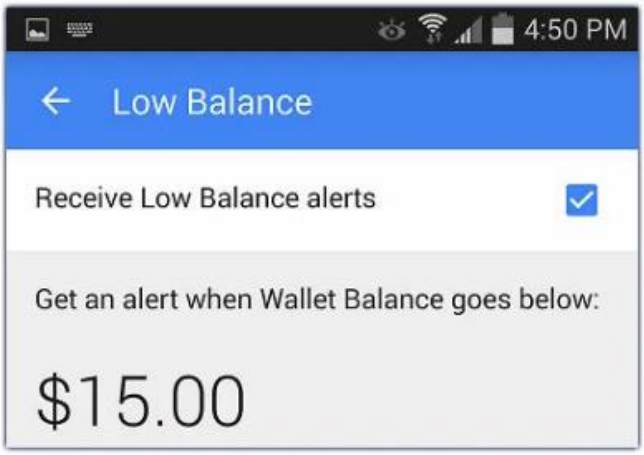
Slika 3.3. Prozor za upisivanje podataka, [16]

Nakon prijave i provjere identiteta od strane *Google*-a, korisniku mora odabrati 4-znamenkasti PIN koji će se u budućnosti autorizirati prilikom svakog ulaska u aplikaciju. Nakon toga poželjno je da korisnik uplati nešto novca na svoje virtualne kartice kako bi se potvrdila njihova valjanost. S tim iznosom korisnik je kasnije u mogućnosti da šalje novac na druge račune, kupuje na internetu ili u trgovinama pomoću mobilnog uređaja i NFC tehnologije.

Osim pomoću mobilnog uređaja korisnik plaćanja može izvršavati pomoću *Google Wallet* kartice koju mora aktivirati i nakon toga mu dođe na kućnu adresu. Kada korisnik plaća pomoću mobilnog uređaja, jednostavno odabere karticu kojom plaća unutar aplikacije i prilikom naplate približi uređaj terminalu za naplatu na udaljenost od 5 cm, zatim upiše svoj PIN i naplata se izvrši [16].

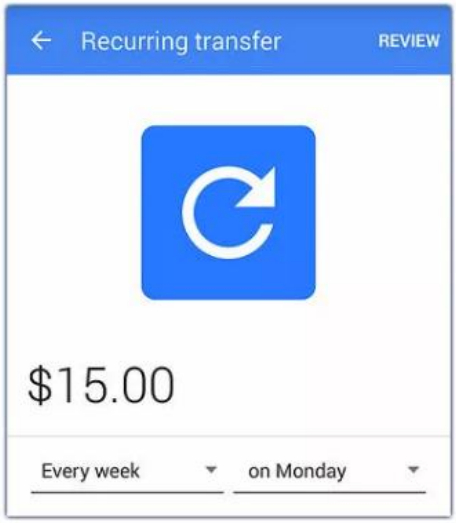
Dodatne funkcionalnosti koje pruža *Google Wallet* aplikacija, osim slanja novca na druge račune, je i upozorenje aplikacije ukoliko je stanje računa nisko iz razloga da bi se izbjegle neugodne situacije prilikom kupovine. Kada iznos na računu

dosegne određenu granicu, aplikacija šalje obavijest korisniku. Korisnik sam može kreirati, postaviti granicu ispod koje želi primati obavijesti odlaskom u postavke aplikacije i odabirom iznosa granice upozorenja kao što pokazuje slika 3.4 [17].



Slika 3.4. Postavka granice upozorenja, [17]

Nadalje, još jedna korisna funkcionalnost je automatsko prebacivanje određenog iznosa na račun. Prilikom dodavanja novca na *Google* račun aplikacija ponudi opciju automatskog punjenja računa. Ova opcija ima smisla za one korisnike kojima su troškovi veliki, i zahtijevaju učestalo obnavljanje računa. Korisnik sam određuje koliki će mu se iznos uplaćivati i na koji dan u tjednu. Prozor sa navedenim postavkama vidi se na slici 3.5 [17].



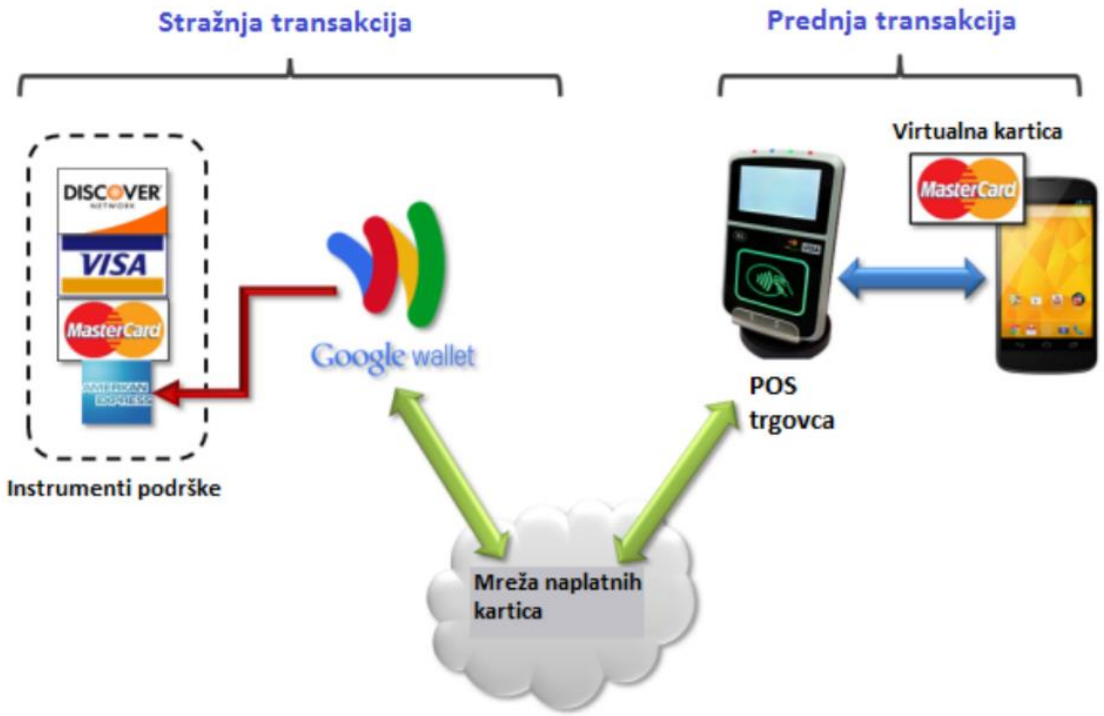
Slika 3.5. Postavke odabira iznosa i dana automatskog punjenja, [17]

2013. godine aplikacija je dobila opciju slanja novca punoljetnim osobama koje posjeduju e-mail, međutim isključivo između američkih korisnika. Opcija slanja je

besplatna kada se šalje s bankovnog računa ili preko *Google Wallet* sustava, ali postoji naknada kada se koristi povezana kreditna ili debitna kartica [17].

3.2.4 Arhitektura Google Wallet aplikacije

Google Wallet zasniva se na ideji da podrži što više kartica u mobilnom novčaniku, što znači da umjesto nošenja svih kartica korisnik ima jedan uređaj koji posjeduje virtualnu karticu. Virtualna kartica u stvarnom vremenu može se preko mreže za naplatu prebaciti na bilo koju od orginalnih kartica. Na slici 3.6 vidi se način funkcioniranja virtualnih kartica kod NFC plaćanja mobilnim uređajima. Korisnik dodaje fizičke kartice u svoj virtualni novčanik na način da na web stranici ili u mobilnoj aplikaciji utipkava broj kreditne kartice, datum istjecanja i CVC2[3]. Detalji o kartici jednoznačno određuju pripadnost kartice korisniku i potvrđuju da on ima pristup njoj. Mogućnost naplate moguća je u bilo kojem trenutku budući da sustav radi 0-24 i da se sve odvija elektronički u stvarnom vremenu, što znači da se sredstva odmah povlače sa kartice.



Slika 3.6. Arhitektura Google Wallet-a i virtualnih kartica, [18]

[3] CVC2 – *Card Verification Code* je sigurnosna šifra, troznamenkasti broj koji se nalazi na poleđini VISA/VISA *Electron/MasterCard/Maestro* kartice, pozicioniran desno od broja kartice [15].

Svaki primjer *Google Wallet* aplikacije ima vlastitu opremu virtualne kartice koja je povezana i sa korisnikom. To je *MasterCard* kartica izdana u ime *Google*-a koja radi na bilo kojem NFC terminalu koji podržava beskontaktno plaćanje, odnosno *MasterCard PayPass* protokol. Kartica ima 16-znamenkasti digitalni broj s prefiksom koji ju povezuje s *MasterCard* mrežom, zatim datum isteka i za NFC transakcije posjeduje kriptografski ključ koji se koristi za generiranje dinamičkog CVC[4]-a.

Prilikom izvršavanja NFC transakcije preko *Google Wallet*-a, platna mreža *MasterCard*-a će sama odrediti put autorizacijskog zahtjeva do *Google*-a, izdavatelja virtualne kartice. *Google* zatim postavlja zahtjev za isplatu sa odabrane kartice sa točnim iznosom, te ovisno o ishodu autorizacije, „*front end*“ transakcija će biti odbijena ili odobrena. Cijela transakcija se odvija u realnom vremenu, budući da se moraju poštivati mrežna pravila o krajnjim rokovima transakcijama koja su vremenski ograničena na nekoliko sekundi [18].

Također, virtualna kartica i stvarni prateći instrumenti mogu biti potpuno odvojeni. Virtualna kartica nije savršena replika orginalne kartice koju korisnik stavlja u svoj novčanik, nema isti datum isteka, ne dijeli isto ime, međutim za NFC transakcije imena korisnika su uređena. Kartice mogu biti na različitim kartičnim mrežama, npr. virtualne kartice mogu biti *MasterCard*, dok se sredstva mogu povlačiti sa *American Express* kartice.

Ovaj sustav može biti kompliciran, i često zna biti na meti prevaranata kada su informacije o kartici spremljene na trgovački terminal ili su poslane na nesiguran način. Kod transakcija kod kojih nije prisutna kartica (CNP[5]) naknada za trgovca je veća nego kod onih kada je kartica prisutna te je ujedno i manje sigurna. Međutim, iako *Google Wallet* aplikacija ne treba fizičku karticu, ona prenosi informaciju kao da je kartica prisutna, pa naknade za trgovce koji posjeduju NFC tehnologiju na svom POS terminalu nisu visoke [19].

[4] CVC – dodatna sigurnost na kartici u obliku broja koji služi za zaštitu od prijevara. služi ako dokaz da korisnik fizički posjeduje karticu u trenutku kupnje [15].

[5] „CNP-transakcija oznacava takve transakcije, odnosno transakcije tokom kojih kartica nije bila fizicki prisutna na prodajnom mjestu (CNP dolazi od engleskog termina *'Card Not Present'*)“ [20].

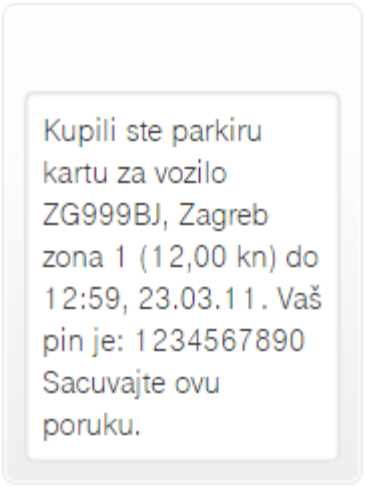
3.3 Mobilno plaćanje pomoću SMS poruka

SMS parking kao jedna od najčešće korištenih usluga s dodanom vrijednosti biti će opisana i objašnjena u dalje u radu. Razvoj telekomunikacijskih usluga i mobilnih sustava uvelike je pomogao u svakodnevnom životu te se počeo koristiti u različitim sferama svakodnevnog života. U prometnom smislu, parkiranje i naplata parkinga ponekad zna stvarati probleme u urbanim sredinama, ponekad zbog žurbe ili nedostatka fizičkog novca korisnik nije u stanju platiti parking. Pomoću mobilnog terminalnog uređaja koristeći usluge dodane vrijednosti SMS-a korisnik je sada i to u stanju. U mnogim gradovima u Hrvatskoj uvedena je ova usluga i do sada pokazala odlične rezultate. Mnogi operateri nude uslugu plaćanja parkinga SMS-om, a u ovom radu će se pokazati na primjeru Hrvatskog telekoma kako to izgleda.

Hrvatski telekom nudi uslugu SMSparking putem SMS-a, na način da korisnik pošalje registracijsku oznaku bez razmaka, interpunkcija i hrvatskih znakova na broj parkirne zone u kojoj se nalazi (ććđžš treba prikazati kao ccdzs). Broj parkirne zone korisnik može saznati na najbližem parkirnom automatu. Primjer SMS-a vidi se na slici 3.7.

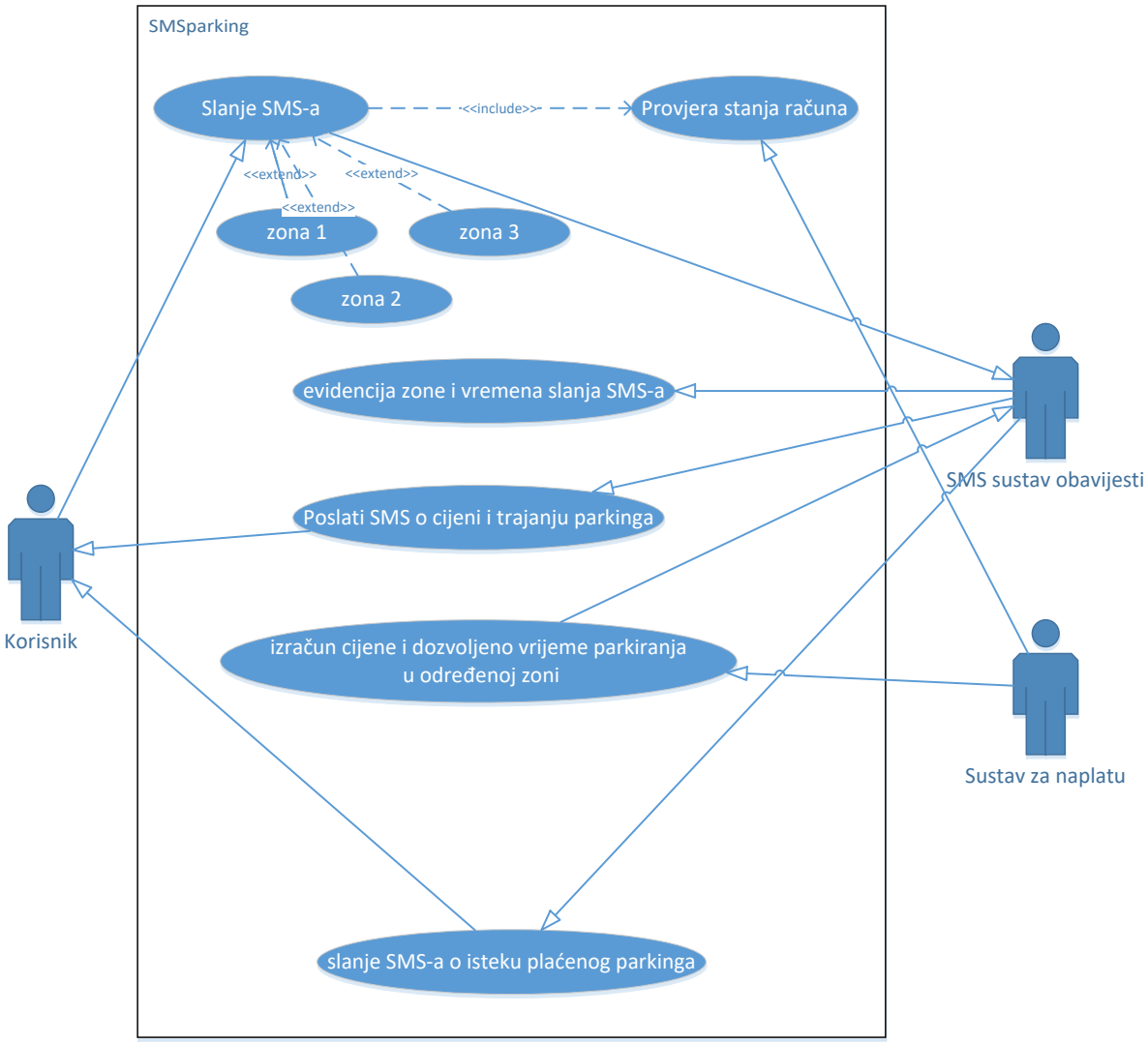
Slika 3.7. SMS zahtjev za naplatom parkinga, [21]

Nakon slanja SMS zahtjeva za naplatom parkinga, korisnik prima SMS poruku s potvrdom i podacima o plaćenom parkiranju (ukoliko ima dovoljno sredstava na računu). Poruku s potvrdom parkiranja koja se vidi na slici 3.8 potrebno je sačuvati za vrijeme trajanja parkiranja jer ona služi kao dokaz o plaćenom parkiranju.



Slika 3.8. SMS poruka s potvrdom parkiranja, [21]

Pet do deset minuta prije isteka parkiranja korisnik dobiva obavijest SMS porukom. Korisnik također može produžiti parkiranje dodatno 1h tako da pošalje SMS sadržaja * ili ponovno upiše registracijsku oznaku na broj odgovarajuće parkirne zone. U svakom trenutku korisnik može provjeriti status svog parkiranja tako da pošalje SMS poruku sadržaja ? na broj odgovarajuće zone. Cijena usluge sastoji se od cijene naknade za izvršenu platnu uslugu (0,65 kn) + cijena parkirne karte (uključuje PDV i ovisi od zone do zone). Dolazne SMS poruke se ne naplaćuju. Kako bi se lakše shvatio proces koji se odvija između korisnika, SMS sustava obavijesti i sustava za naplatu napravljen je dijagram slučaja uporabe prikazan na slici 3.9.



Slika 3.9. Dijagram slučaja uporabe za SMSparking

Hrvatski telekom također nudi mogućnost plaćanja parkiranja SMS-om u javnim garažama. Prilikom ulaska u garažu korisnik jednostavno uzme parkirnu karticu iz automata, i prati upute za plaćanje putem SMS poruke. Prije izlaska iz garaže kao sadržaj poruke ukuca se serijski broj kartice i pošalje na broj garaže. Potvrdni SMS sadržavati će plaćeni iznos parkiranja, vrijeme do kada je potrebno izaći iz garaže i jedinstveni PIN za slučaj reklamacije. Ukoliko potvrdni SMS nije stigao u roku od 2 min, plaćanje uslugom SMSparking nije uspjelo, te se niti korisnički račun neće teretiti [21].

Treća usluga koja se bazira na SMS mobilnom plaćanju je SMSbon. SMSbon je usluga kojom se račun može nadoplatiti bonovima od 27.5 kn, 55 kn, 110 kn i 220 kn. Ukoliko se usluga koristi bez unosa koda, sadržaj poruke koji se šalje treba izgledati ovako: iznos kuna kojim korisnik želi nadoplatiti račun te znak „#“ zatim telefonski broj

kojim želi nadoplatiti i znak „#“, te iza toga može napisati poruku od najviše 90 znakova. Ukoliko se usluga koristi sa unosom koda jednostavno se pošalje iznos kojim se želi nadoplatiti račun na broj „13240“ i prate se daljnje upute. Cijena ove usluge se ne naplaćuje dodatno kao npr. SMSparking, kao niti poslane ni primljene poruke vezane uz nadoplatu računa.

Četvrta usluga temeljena na SMS je VAS SMS. Omogućava personaliziran i brz komunikacijski kanal za interakciju operatora sa korisnicima, informiranje i obavještavanje korisnika o aktualnim ponudama, servisnim informacijama, organiziranje i provođenje raznim nagradnih igara i kvizova, SMS chat-a, promoviranje proizvoda i usluga.

Uz SMS usluge koje su objašnjene Hrvatski telekom nudi još i: SMS redomat, SMSprijevoz, SMSflert, SMSrelaks, SMSinfo i Dajnazovi. Neke od njih se dodatno naplaćuju, a neke ne [21].

3.4 Mobilno plaćanje pomoću bluetooth tehnologije

Mobilno plaćanje je trenutno važna tema što se tiče mobilnog poslovanja i aplikacija vezanih uz to. Kako sve više poduzeća i trgovaca daje pozornost mobilnim korisnicima što se tiče prodaje proizvoda i usluga, tako postoji velika potražnja za dobavljačima koji će omogućiti pouzdane i jednostavne mobilne sustave za sigurno i učinkovito plaćanje. *Bluetooth* uređaji koriste radio valove da bi se spojili na mobilni uređaj ili računalo umjesto preko klasičnih žica. Osim mnogih praktičnih primjena u svakodnevnom životu (telefoniranje i vožnja u isto vrijeme bez upotrebe ruku za držanje mobitela) razne kompanije su shvatile da bi *bluetooth* tehnologija mogla pronaći svoju primjenu u području mobilnog plaćanja.

Kod mobilnih plaćanja koja koriste *Bluetooth* tehnologiju informacije se prenose pomoću radiovalova. Za mobilna plaćanja, programeri su razvili senzore koje pokreću male baterije. Budući da ti senzori koriste vrlo malo energije u odnosu na normalne ovaj standard za mobilna plaćanja naziva se još i BLE (*Bluetooth Low Energy*).

BLE je pametno korištenje bluetooth veze u smislu da se koristi što manje energije uređaja na kojem se koristi za prijenos podataka. BLE zapravo omogućava

bežični prijenos podataka kao i klasični bluetooth, međutim fokus je na što manjoj potrošnji energije. Malu potrošnju energije određuju sljedeći faktori:

- povećano vrijeme mirovanja (*sleep time*),
- brze konekcije,
- niska maksimalna energija.

Kada korisnik želi otići u trgovinu i platiti određeni proizvod sa svojim mobilnim uređajem, senzori prepoznaju BLE tehnologiju u mobilnom uređaju te se povezuju s njim. Budući da BLE tehnologija radi na udaljenosti do 50m , korisnik može doslovno samo prošetati pokraj blagajne, i sustav naplate će automatski odraditi plaćanje, bez da korisnik uopće izvadi mobitel iz džepa.

Glavne razlike između BLE i NFC tehnologije su:

- i BLE i NFC su tehnologije kratkog dometa i rade na bežičnom principu, ali BLE radi na malo većem dometu pri čemu se povećavaju pogodnosti samog korištenja,
- brzina prijenosa podataka je brža kod NFC-a ,
- NFC omogućava razmjenu podataka isključivo između dva uređaja (*one-to-one),* dok BLE može istovremeno ostvariti višestruke konekcije [22].

S obzirom na mobilne transakcije BLE omogućava tri scenarija kod plaćanja:

1. U prvom scenariju postoji virtualna kartica koja je pohranjena u mobilnom uređaju koji je spojen preko BLE na POS terminal koji je dalje povezan sa platnom mrežom.
2. U drugom scenariju podaci su pohranjeni u *cloud*-u[6]. Preko BLE telefon se spaja na POS *beacon* uređaj koji se onda dalje povezuje s *cloud*-om. Ovaj scenarij omogućuje personalizaciju pri ulasku kupca u trgovinu, gdje se njegov mobilni uređaj automatski povezuje sa BLE *beacon*-om, te se fotografija i ime kupca šalju na blagajnu. Transakcija ne zahtijeva karticu i gotova je kada blagajnik odradi prepoznavanje lica kupca i potvrde koju je dobio od kupca.

[6] *Cloud* – pohrana dokumenata, fotografija, videa i drugih datoteka na web stranicu – da biste u konačnici sadržaj mogli jednostavnije dijeliti sa drugima, ili da biste sebi osigurali osiguranu kopiju. Svemu što pohranite možete pristupiti sa bilo koje lokacije ili bilo koje vrste uređaja (laptopa, mobitela, tableta i sl.).

3. U trećem scenariju uključeni su podaci o samom mobilnom uređaju, koji je povezan preko BLE sa POS uređajem, a POS uređaj je dalje spojen sa platnom mrežom. Ovaj scenarij omogućuje kupcima da samostalno skeniraju proizvode [22].

Slika 3.10. Različite vrste Beacon uređaja, [23]

Na slici 3.10 mogu se vidjeti različiti oblici i dimenzije *Beacon* uređaja, međutim oni su uvijek dovoljno mali da stanu na skrivena mjesta, a da opet imaju svoju funkciju.

U usporedbi sa NFC-om, glavna prednost koju nudi BLE je zapravo sloboda i fleksibilnost plaćanja. Uz veći domet, BLE također ima brže vrijeme procesiranja. Potrebno je samo 0.003 sekunde da bi se obavila transakcija pomoću BLE tehnologije. U usporedbi sa NFC tehnologijom, kojoj je potrebno 0.1 sekunda za transakciju, pa razlika u vremenu čini BLE transakcije gotovo trenutnim. Omogućuje spajanje na POS uređaj bilo gdje u trgovini. NFC u drugu ruku zahtijeva neposrednu blizinu POS uređaja da bi funkcionirao. Isto tako BLE *beacon* omogućava da mobilne aplikacije koje posjeduju trgovci budu u mogućnosti slati prilagođene ponude na korisničke mobilne uređaje kada su sami korisnici u blizini, dok to NFC tehnologija nikako ne može postići. BLE tehnologija zahtijeva mnogo manje ulaganje u POS tehnologiju, a kompatibilna je u beskontaktnom okruženju. Korisnik BLE tehnologije ne mora čekati u redu da bi obavio plaćanje, kao kod NFC tehnologije koja zahtijeva neposrednu blizinu POS uređaja [24], [22].

Što se tiče sigurnosti BLE tehnologije, budući da su POS *beacon* uređaji koji detektiraju druge uređaje u blizini i šalju isključivo odlazne signale, nema opasnosti kod transakcije. U drugu ruku, rizik leži u aplikacijama koje koriste ove signale, pa u tom smislu ova tehnologija nije nista bolja niti lošija od drugih lokacijskih sustava koji komuniciraju preko mobilnih uređaja. Nadalje, lokacijski sustavi koji osiguravaju sesiju prilikom transmisije podataka kao NFC, generalno se smatraju sigurnijima kada su u pitanju mobilna plaćanja [25].

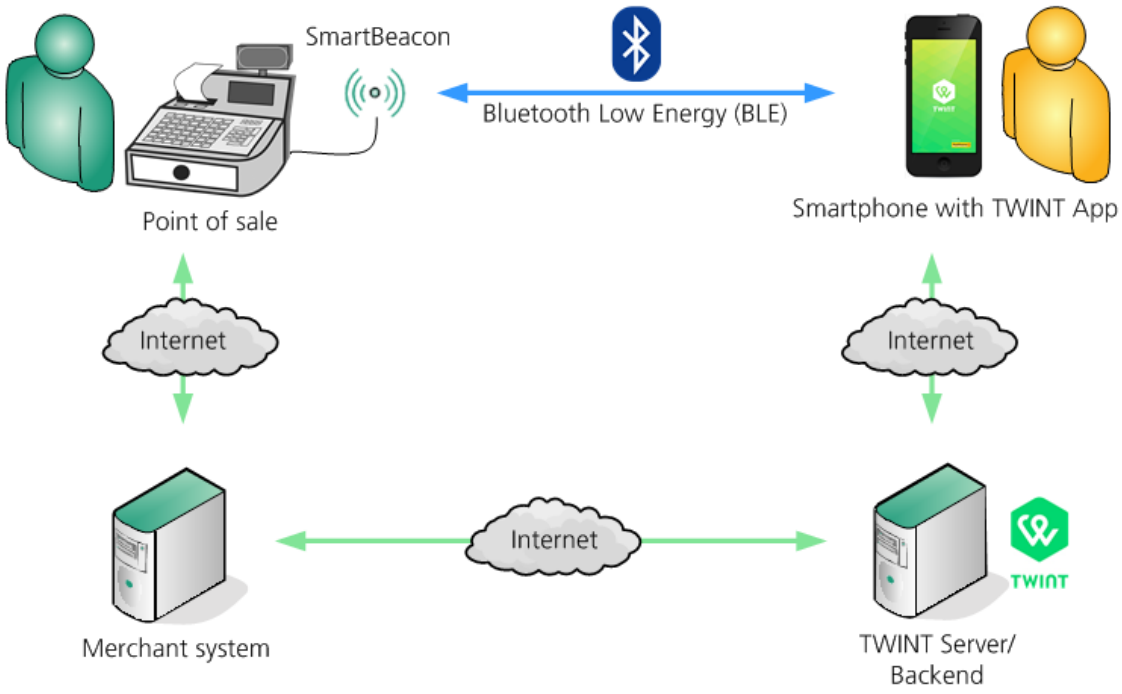
TWINT je aplikacija koja omogućava plaćanje na mjestu prodaje preko *beacon* uređaja uz pomoć BLE tehnologije, ili ukoliko se radi o online kupovini preko QR koda ili tokena. U tim procesima TWINT automatski uzima podatke o *loyalty* karticama i digitalnim kuponima kupca, dok prodavači također imaju benefite od aplikacije u smislu da mogu promovirati svoje kupone i vaučere individualno, i na točno ciljanu populaciju. TWINT u odnosu na ostale slične aplikacije omogućava kupcima da uopće ne moraju imati bankovne račune ili debitne kartice. Rješenje radi neovisno o kojem se telekomu, davatelju usluge radi i može biti instaliran na bilo koji *iOS* ili *Android* operativni sustav. Sve što korisnik treba napraviti je registrirati se pomoću mobilnog broja, napuniti *prepaid* karticu i obaviti prvo plaćanje [26].

TWINT aplikacija se temelji na BLE i beacon tehnologiji. Uz to što je BLE jako štedljiv način korištenja energije, u odnosu na NFC tehnologiju BLE mogu koristiti i korisnici *iPhone* mobilnih uređaja što nije slučaj kod NFC-a. Slično kao i kod NFC-a, proces plaćanja TWINT aplikacije traje svega 3-5 sekundi. Kod plaćanja, prodajno mjesto ne komunicira direktno sa korisničkim mobilnim uređajem, već se spaja sa TWINT aplikacijom, ali indirektno, u pozadini. Osim *beacon* uređaja koji mora biti spojen sa USB kablom, niti jedan dodatni *hardver* ne mora biti instaliran na samom mjestu prodaje. Svejedno, blagajna (mjesto prodaje) mora biti spojena internet vezom sa trgovinskim sustavom u cilju da bude sposobna komunicirati sa TWINT serverom (kriptirano). Serveri zauzvrat komuniciraju sa TWINT aplikacijom na korisnikovom mobilnom uređaju. Ako mobilni uređaj nema pristup internetu, blagajna služi kao komunikacijski kanal između aplikacije i TWINT servera [26].

Proces naplate na blagajni putem beacon uređaja može se u grubo podijeliti u dvije faze: tzv. uparivanje i stvarna naplata. Uparivanje ima na raspolaganju sljedeće sustave (korisnički mobilni uređaj, TWINT server i sustav prodaje samog trgovca)

kako bi točno identificirala koji korisnik se nalazi na kojem prodajnom mjestu. Za tu svrhu korisnik otvara svoju TWINT aplikaciju i postavlja svoj mobilni uređaj kratko pokraj *beacon* uređaja. Ovaj proces se obično obavlja prije ukupnog iznosa. Ovo rano uparivanje, u kojemu informacije o *loyalty* karticama i kuponima mogu biti već poslane, omogućava brži proces u drugoj fazi, plaćanju. *Beacon*-ovi prijenosni oglasni paketi, uključujući i *beacon* ID, mogu biti detektirani do 2m udaljenosti.

Međutim, raspon TWINT aplikacije postavljen je tako da se uparivanje događa isključivo onda kada je mobilni uređaj u blizini (nekoliko cm udaljenosti). Jednom kada je uparivanje pokrenuto, *beacon* prestaje sa slanjem oglasnih paketa, i niti jedan drugi mobilni uređaj ne može se spojiti na *beacon*. Tako blagajna može posluživati samo jednog korisnika u vrijeme procesa plaćanja, i na taj način je proces plaćanja zaštićen od smetnji uzrokovanih drugim mobilnim uređajima i korisnicima. Na slici 3.11 vidimo pojednostavljeni prikaz rada TWINT sustava i relacije između sudionika [26].



Slika 3.11. Prikaz rada TWINT sustava, [26]

TWINT aplikacija šalje primljeni *beacon* ID prema TWINT serveru. Server identificira blagajnu i korisnika koji može biti dodijeljen u pozadini. Nakon toga, server vraća potvrdnu poruku prema mobilnom uređaju, koja se pokazuje u aplikaciji. U isto

vrijeme blagajna zahtijeva korisničke *loyalty* podatke od TWINT sustava. Nakon uparivanja, pokrenuto plaćanje dalje se pokreće kada prodavač odluči putem TWINT-a. U ovoj fazi plaćanja fokus je na prebacivanju iznosa sa korisničkog TWINT računa na prodavačev TWINT račun. Transakcija započinje kada prodavač pošalje zahtjev za plaćanjem sa iznosom i valutom prema TWINT-u. Zbog postojećeg uparenja, korisnik koji mora platiti iznos poznat je na serveru i odgovor se šalje prema TWINT aplikaciji. Odgovor prikazuje iznos koji se plaća uz podatke o trgovcu. Ovisno o korisničkim sigurnosnim postavkama, sustav direktno autorizira plaćanje ili korisnik iznos potvrđuje ručno ili unosom PIN-a, a TWINT aplikacija prosljeđuje sve dalje u pozadinu. Transakcija je zatim gotova na TWINT serveru i blagajna može čekati pitanje o status plaćanja, no zapravo i na blagajni i na TWINT aplikaciji ispisuje se poruka o uspjehu ili neuspjehu transakcije pa je sve transparentno [26].

Sigurnost u TWINT-u postiže se arhitekturom sustava i korištenjem posebnih *SmartBeacon*-a. Sustav je napravljen tako da se osjetljivi podaci ne prenose preko *beacon*-a. Beacon jednostavno samo određuje kojem trgovcu i na kojoj blagajni korisnik želi platiti. Sve sigurnosno orjentirane transakcije vođene su u pozadini, te su zaštićene prema vodećim bankarskim standardima. Identitet *beacon*-a (*beacon* ID), koji se šalje pomoću *beacon*-a u paketskim oglasima, sačinjen je od UUID, odnosno glavnog i sporednog ID-a. Uz pomoć *SmartBeacon*-a može se konfigurirati ovakav *beacon* ID. Dodjeljuje se blagajni prilikom registracije i može biti promijenjen u konzultacijama sa trgovcem u bilo kojem trenutku. *Beacon* memorija sadrži privatni ključ koji se koristi za sigurnosnu identifikaciju *beacon*-a. Identitet je potvrđen uz pomoć izazov-odgovor procedure. Ukoliko se *beacon* ukrade, privatni ključ i *beacon* ID budu izgubljeni budući da se prekine dovod energije preko USB ulaza. Gubitak podataka je ograničen isključivo na hardverski dio, odnosno sustav ne gubi podatke [26].

4 QR KODOVI

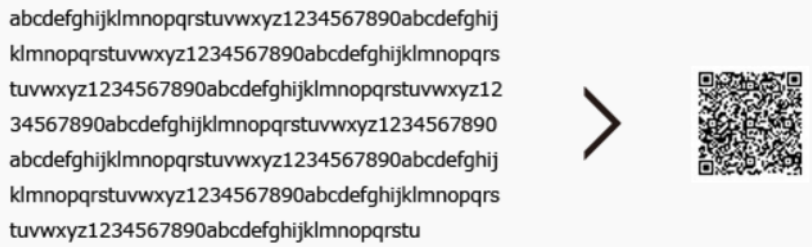
Kao što je navedeno ranije u radu (u potpoglavlju „Klasifikacija elektroničkog poslovanja“) u ovom diplomskom radu naglasak će biti na elektroničkom poslovanju koje se bazira na QR kodovima. U ovom poglavlju opisati će se opće odrednice, povijest nastanka tehnologije, vrste kodova i način rada. Također napraviti će se i anketa da bi se ispitalo kolika je zastupljenost ove tehnologije u stvarnim situacijama.

4.1 Općenito o QR kodovima

QR kod je dvodimenzionalni barkod dizajniran od strane *Denso Wave Company*, originalno je dizajniran za praćenje dijelova kad se kreću velikom brzinom pokretnom linijom. QR kod sastoji se od crno bijelo kvadratića, a najveća primjena im je za pretvaranje koda u korisnu informaciju [27].

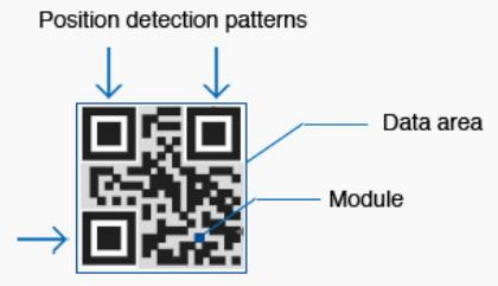
QR kodovi doprinose stvaranju raznolikosti ljudskih aktivnosti kod kuće, ali i na radnom mjestu. Mogu se koristiti u svakodnevnom životu ne samo za određene tiskane stvari kao letke i kartice, već isto tako i kao sustav plaćanja. Također QR kodovi se uvelike koriste za različite poslovne namjene u tvornicama i logističkim centrima. Budući da su se toliko proširili u svim komponentama svakodnevnog života, postali su nezamjenjiv alat u ljudskim životima. Upravo ta visoka funkcionalnost koja je u skladu s današnjim načinom života javno se vrednuje, a 2012. godine nagrađena nagradom *Good Design Award* pod pokroviteljstvom Japanskog instituta za promociju dizajna [28].

QR kodovi imaju visoki kapacitet što se tiče pohrane podataka. Dok su konvencionalni bar kodovi sposobni primiti otprilike 20 znamenaka, QR kod je sposoban upravljati sa nekoliko desetaka do nekoliko stotina puta više informacija. QR kod je sposoban upravljati i pohraniti sve tipove podataka, kao što su brojevi i abecedni znakovi, Kanji, Kana, Hiragana, simboli, binarni i kontrolni kodovi. U jedan simbol može se kodirati čak do 7089 znakova [28].



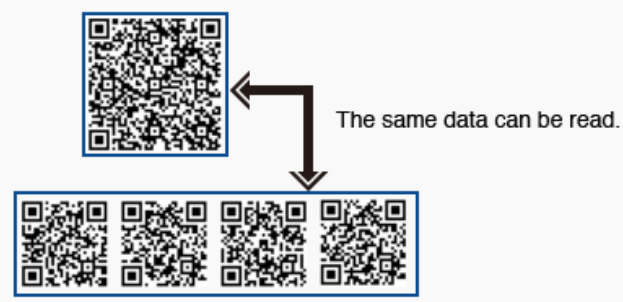
Slika 4.1. Primjer QR koda, [28]

Na slici 4.1 može se vidjeti kolika veličina QR koda je potrebna da bi se na njega spremilo 300 alfanumeričkih znakova. Otkad je napravljeno da QR kod može nositi informaciju i horizontalno i vertikalno, QR kod je sposoban primiti istu količinu podataka u otprilike desetinu prostora tradicionalnog barcoda. Isto tako je moguće napraviti i *Mikro* QR kod ukoliko je stvar na koju se stavlja izrazito mala. Kako je dizajniran u Japanu, napravljeno je da može spremiti JIS *Level* 1 i *Level* 2 kanji set znakova. Kodna riječ je jedinica koja gradi područje podatkovnog prostora, i u slučaju kod QR kodova, jedna kodna riječ odgovara 8 bit-a. QR kod je moguće pročitati u svim smjerovima (360 stupnjeva) sa velikom brzinom čitanja. QR je u mogućnosti to raditi zbog uzoraka za detekciju položaja koji se nalaze u tri ugla na samom simbolu kao što se vidi na slici 4.2. Ovi uzorci za otkrivanje položaja omogućavaju stabilnu brzinu čitanja, zaobilazeći negativne učinke pozadinskih smetnji [28].



Slika 4.2. Uzorci za otkrivanje položaja, [28]

QR kodovi mogu biti podijeljeni u više podatkovnih površina, kao i što se informacije pohranjene u više simbola QR kodova mogu spojiti u jedan podatkovni simbol. Jedan podatkovni simbol može se podijeliti na čak 16 manjih simbola, što zapravo omogućuje ispis u uskim područjima kao što je prikazano na slici 4.3 [28].



Slika 4.3. Mogućnost dijeljenja i spajanja QR kodova, [28]

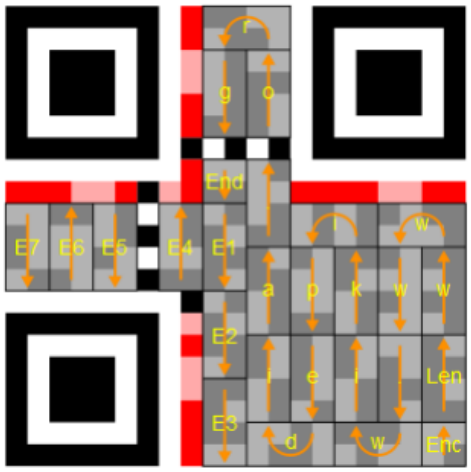
Ovi dvodimenzionalni kodovi omogućavaju brz prijenos podataka pomoću mobilnog uređaja i pravovremeni pristup relevantnom i korisnom sadržaju u postupku kupovine. Zahvaljujući praktičnosti i dostupnosti korisniku, postoje različite mogućnosti korištenja QR kodova u različite svrhe. QR kodovi mogu biti postavljeni na razne omote proizvoda, letke, brošure, kataloge, novine, pozivnice, čestitke itd., omogućavajući korisnicima da dobiju informacije o proizvodu, ili da ih kod odvede na internetsku stranicu koja je vezana uz taj objekt. Također se može koristiti i za mobilna plaćanja [29].

QR kodovi kategorizirani su u 40 verzija ovisno o broju modula koje sadrže s obzirom na svoje dvije dimenzije pa tako postoji raspon između verzija 1 (sastoji se od 21x21 modul) do verzije 40 (koja se sastoji od 177x177 modula) s tim da svaka sljedeća verzija ima četiri modula više nego prethodna. Trenutno najkorištenija je verzija 6 (41x41 modul) budući da se može lako pročitati pomoću većine mobilnih aplikacija, a i može pohraniti dovoljno podataka. Moduli na QR kodu mogu se podijeliti u dvije skupine: funkcionalne oznake i kodirajuća polja. Funkcionalne oznake kao što je ranije navedeno u radu, služe kako bi kamera na mobilnom uređaju prepoznala QR kod, dok kodirajuća polja sadržavaju podatke (informaciju), kod za ispravljanje pogrešaka te informaciju o verziji i formatu koda [29].

Kako je ranije navedeno, QR kod ima sposobnost ispravljanja pogrešaka u 4 nivoa koristeći algoritam *Reed-Solomona*[7]. Prema tome algoritmu QR kodovi sadrže validacijske podatke pohranjene u informacijama koje omogućavaju ispravno čitanje koda bez obzira što maksimalno 7%, 15%, 25% ili 30% koda fali, ili je oštećeno, ili je netočno [29].

[7] Reed i Solomon su 1960. godine opisali na sistematičan način pisanja kodova koji mogu detektirati i ispraviti višestruke slučajne pogreške [29].

Najveći dio QR koda je rezerviran za kodiranje same poruke. Postupak kodiranja poruke je jednostavan i pokazati će se na jednom primjeru. Na slici 4.4 prikazuje se proces čitanja QR koda koji kao poruku ima zapisanu web adresu www.wikipedia.org [34].



Slika 4.4. Proces čitanja QR koda, [34]

Na slici 4.4 vide se standardni elementi svakog QR koda koji su opisani i objašnjeni ranije (veliki kvadrati na rubovima i podaci o razini korekcije pogrešaka). Poruke koje su kodirane u QR kodu sastoje se od:

- Vrste kodiranja (brojke, alfanumerički znakovi..),
- Duljine poruke,
- Poruka
- Oznaka kraja poruke,
- Korekcijskih kodova.

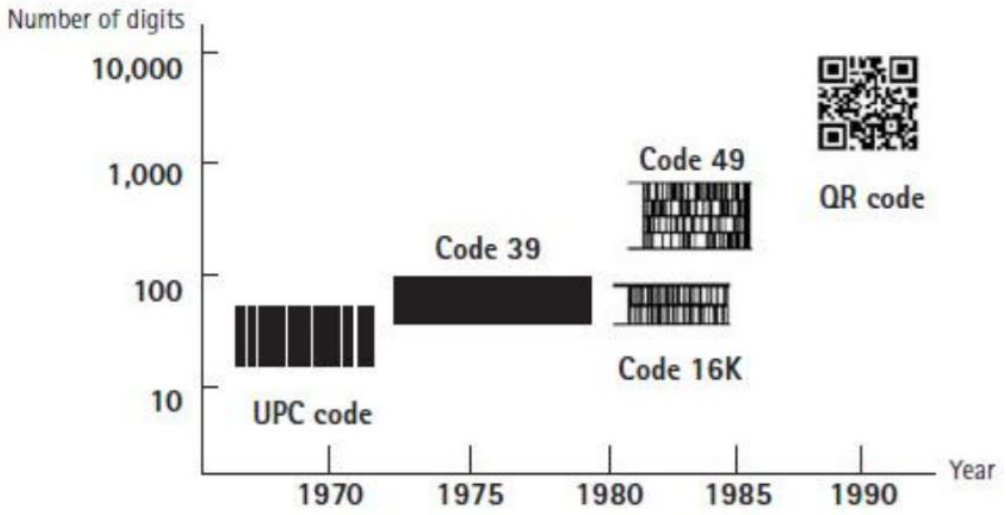
Svi navedeni dijelovi promatraju se kao jedinstven niz jedinica i nula koje treba upisati u QR kod i na njih se primjenjuje maska. Maska je funkcija koja određuje hoće li neki bit poruke biti 1 ili 0 zavisno o njegovoj koordinati unutar QR koda. Prilikom kodiranja poruke 1 se prikazuje kao crni modul ili ukoliko se radi o 0 modul će biti bijeli. Skener poruku čita dva stupca prema gore do vrha koda, potom dva stupca prema dolje i tako do kraja koda. Na slici 4.4 je smjer skeniranja označen strelicom. Skener prvo pročita vrstu kodiranja, na slici označeno slovima „Enc“, potom pročita duljinu poruke (na slici označeno slovima „Len“). Zatim se poruka čita znak po znak, budući da je skener prvo pročitao vrstu kodiranja zna kako pročitati svaki znak

poruke. U ovom slučaju radi se o alfanumeričkoj poruci gdje se 8 bita koristi za jedan znak. Poruka je: www.wikipedia.org. Nakon poruke skener čita oznaku za kraj i korekcijske kodove [34].

4.2 Povijest nastanka QR kodova

Tijekom 1960-tih kada je Japan doživio veliki ekonomski rast, u supermarketima prodavalo se svašta, od hrane do odjeće i obuće. Blagajnici bi pri svakoj kupnji svaku šifru od željenog proizvoda morali utipkati ručno, te su zbog toga patili od bolnih zglobova. Izum barkoda riješio je taj problem, budući da se od tada svaki proizvod skenirao pomoću optičkog senzora gdje se informacija o istom slala na zaslon računala. Najveći problem je bio što je barkod mogao pohraniti samo 20 alfanumeričkih znakova. Korisnici su kontaktirali *Denso Wave* koji su proizvodili barkode čitače i pitali ih da li je moguće napraviti barkod koji bi mogao pohraniti više informacija. Potaknuti tim zahtjevima, *Denso Wave* razvija novi dvodimenzionalni kod. Godinu i pol nakon početka projekta, i nakon mnogih pokušaja i pogrešaka, QR kod je bio sposoban pohraniti do 7000 znakova i mogao se čitati 10 puta brže od ostalih kodova [28].

Faza razvoja, odnosno evoluciju QR koda najbolje prikazuje slika 4.5. Na slici se vidi da su 1970. godine razvijeni UPC simboli koji su sadržavali 13 znakova, te su imali mogućnost direktnog unosa u računalo. Zatim, 1974. godine razvijen je *Code* 39, koji je mogao pohraniti 30 alfanumeričkih znakova. Nakon toga 1980-tih razvijen je kod 16K i kod 49, te 1994. godine razvijen je QR kod koji je mogao pohraniti 7000 znakova uključujući i Kanji (kineske znakove) [27].



Slika 4.5. Evolucija QR koda, [27]

Tvrtka *Denso Wave*, izumitelj QR koda, odlučila je kako neće staviti zabranu na svoj patent što je dovelo do razvoja međunarodnog standarda ISO/IEC 18004:2006, te budući da je specifikacija otvorena, omogućeno je svim programerima da izrađuju nove tipove QR koda [27].

Svoje veliko širenje u javnosti QR kod je doživio 2002. godine u Japanu, kada su ljudi počeli kupovati mobilne uređaje sa opcijom čitanja QR kodova. Kako se QR kod širio globalno, novi tipovi QR koda su se stvarali kako bi zadovoljili nove sofisticirane potrebe korisnika. *Mikro* QR kod je također napravljen da bi se zadovoljile potrebe stavljanja koda na male stvari na malom prostoru [28].

4.3 Vrste QR kodova

Postoji dosta različitih vrsta, odnosno modela QR kodova koji se razlikuju prema izgledu, ali i prema funkcionalnostima koje posjeduju. U nastavku će se predstaviti svaki od njih sa nekim svojim specifičnostima.

4.3.1 QR kod Model 1 i Model 2

Model 1 predstavlja originalni QR kod, kod koji je sposoban pohraniti 1,167 znakova sa svojom najvećom verzijom 14 koja ima dimenzije 73x73 modula. Izgled Modela 1 može se vidjeti na slici 4.6 [28].

Slika 4.6. QR kod Model 1, [28]

Model 2 je kreiran poboljšavanjem Modela 1, njegova prednost je što se čita još lakše čak i ako je sam kod iskrivljen u nekom smjeru. QR kodovi koji se ispisuju na iskrivljenim površinama, ili čija se slika prilikom čitanja izobliči zbog kuta čitanja mogu se učinkovito čitati tako da ima se ugradi uzorak poravnavanja. Izgled Modela 2 može se vidjeti na slici 4.7 [28].

Slika 4.7. QR kod Model 2, [28]

Ovakav kod može pohraniti do 7089 uzoraka u svojoj najvećoj verziji 40 gdje ima dimenzije 177x177 modula [28].

4.3.2 Micro QR kod

Glavna značajka *Micro* koda je da ima samo jedan uzorak za detekciju položaja u usporedbi s redovitim QR kodom koji zahtijeva određenu količinu mjesta na kodu budući da se uzorci za detekciju položaja nalaze na tri ugla simbola. Nadalje, QR kod zahtijeva barem 4 modula široku marginu oko simbola, dok su kod *Micro* QR koda dovoljna i 2 modula. Upravo takva konfiguracija Micro QR koda omogućava ispisivanje u područjima manjim od samog QR koda. Razlike između QR koda i *Micro* QR koda mogu se vidjeti na slici 4.8 [28].

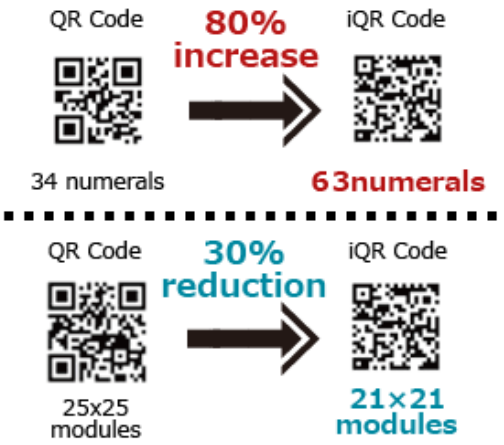
Slika 4.8. Usporedba Micro QR i QR koda, [28]

Količina podataka koja može biti pohranjena na *Micro* QR kod nije jako velika, a iznosi oko 35 znakova. Budući da ova vrsta može učinkovitije šifrirati podatke od redovitog QR koda, njegova veličina ne mora biti puno veća budući da se količina pohranjenih podataka povećava, za razliku od slučaja s redovnim QR kodom [28].

4.3.3 iQR kod

iQR kod je matrični tip 2D koda koji omogućava jednostavno čitanje položaja i veličine. Ovaj kod dopušta širok raspon kodova, od onih manjih od tradicionalnih QR kodova i *Micro* QR kodova, do velikih koji mogu pohraniti više od tih istih. Ovaj kod može se tiskati u pravokutnom obliku, kao preokrenuti kod, crno bijeli inverzni kod ili kao kod točkastog uzorka što omogućuje primjenu u različitim aplikacijama te u različitim područjima [28].

iQR kod može pohraniti veću količinu informacija nego tradicionalni QR kod. iQR kod iste veličine kao tradicionalni QR kod može pohraniti 80% više informacija, a ukoliko bi bila pohranjena ista količina informacija, iQR kod može biti i do 30% manji u odnosu na tradicionalni. Na slici 4.9 može se vidjeti usporedba iQR i tradicionalnog koda u vidu količine pohranjenih informacija i veličine koda [28].



Slika 4.9. Usporedba iQR i tradicionalnog QR koda, [28]

Sa iQR kodom mogu se generirati kodovi koji mogu sadržavati puno više informacija nego što je to moguće sa QR kodom kao što je prikazano na slici 4.10. Broj znakova koji se mogu pohraniti sa najvećom verzijom QR koda je oko 7000 znakova, dok je sa iQR kodom taj broj puno veći. Najveća verzija iQR koda ima dimenzije 422x422 modula i može pohraniti do 40 000 znakova. iQR kod ima veću sposobnost obnavljanja od tradicionalnog QR koda [28].

Slika 4.10. Usporedba razine korekcije između QR i iQR koda, [28]

Razina ispravljanja pogrešaka iznosi do 30% cijelog koda za QR kod, što znači da je moguće povratiti kod sa ovim postotkom oštećenja. Za iQR kod, taj postotak se povećava na čak 50% [28].

4.3.4 SQRC

SQRC je vrsta QR koda opremljena sa funkcijom ograničavanja čitanja. Prigodan je za korištenje i pohranu privatnih podataka i za upravljanje internim informacijama neke tvrtke i slično. SQRC kod može se očitavati isključivo sa

određenim specifičnim tipovima skenera, međutim ova funkcionalnost ne garantira da će kodirani podaci biti sigurni. Podaci koji se pohranjuju SQRC kodom sastoje se od javnog i privatnog dijela, a uz SQRC je također moguće pohraniti 2 kontrolne razine podataka u jednom kodu. Izgled SQRC koda ne razlikuje se od tradicionalnog QR koda. Funkcionalnosti koje dolaze sa tradicionalnim QR kodom, ispravljanje pogrešaka, zadržavaju se i kod SQRC koda [28].

4.3.5 Frame QR

Frame QR kod je QR kod sa „slikarskim platnom“ u sebi koje se može koristiti na različite načine. U središtu ovog koda nalazi se područje platna gdje se na različite načine mogu urediti slike, slova i još puno toga, što omogućuje postavljanje koda bez gubitka dizajna ilustracije, fotografije itd. kao što se vidi na slici 4.11 [28].

Slika 4.11. Primjeri predložaka Frame QR kodova, [28]

Područje platna ne ometa čitanje kodova, a oblik i veličina platna može se odrediti iz predložaka ili može biti određena prema želji korisnika [28].

4.4 Primjena QR kodova

Zbog svog jednostavnog dizajna i velike nosivosti informacija, QR kodovi su našli široku primjenu u različitim područjima poslovnog svijeta. Kada se kupac raspitivao za podatke vezane uz proizvod, mnogo se vremena trošilo na to da se istraži to sve. Da bi se riješio taj problem, QR kodovi počeli su se ljepiti na proizvode, odnosno kutije koje su dolazile u tvornice. Svi podaci (datum proizvodnje, mjesto podrijetla, težina, broj serije), vezani uz taj proizvod ili sirovinu bili su zapisani u QR kodu. Čim su proizvod ili sirovina stigli u tvornicu očitavanjem njihovih QR kodova znalo se šta dalje sa njima raditi, odnosno da li ih spremiti u skladište, ili idu u

proizvodnju. Također pomoću QR kodova lakše se vodila evidencija skladišta i njegovo pražnjenje (FIFO[8]), povijest proizvoda, popis proizvoda u dućanu [28].

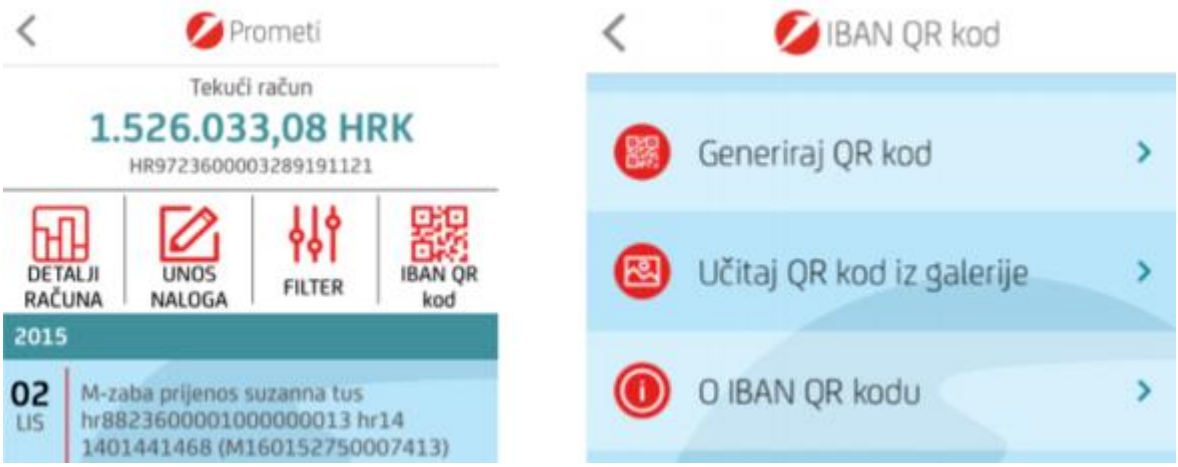
Kako se razvijala tehnologija, internet i telekomunikacije, QR kodovi su se počeli koristiti i u druge svrhe: kao linkovi za povezivanje na internetske stranice, kao kuponi za određene akcije, kao karte za koncerte ili neka druga društveno kulturna događanja, sredstvo prijenosa informacija u svrhu plaćanja/prijenosa novca, te za razne mobilne aplikacije. Kako se u ovaj rad bavi mobilnim elektroničkim poslovanjem, malo će se detaljnije opisati primjena QR koda u svrhu plaćanja ili prijenosa novca. Postoji puno aplikacija i sustava koji koriste QR kod u svrhu prijenosa novca ili plaćanja, a ovdje će se opisati Erste Wallet i m-zaba aplikacije.

Erste Wallet aplikacija omogućava svojim korisnicima da koriste mobitel prilikom plaćanja, slanja i primanja novca. Aplikacija nudi i opciju korištenja različitih računa te praćenja povijesti transakcija, kao i pregled stanja računa bila kada i bilo gdje. Prije ulaska u aplikaciju korisnik mora unijeti svoj PIN kako bi pristupio funkcijama koje nudi aplikacija. Kada korisnik uđe u aplikaciju ima opciju plaćanja gdje koristi kameru mobilnog uređaja i uz pomoć aplikacije skenira QR kod koji mu je pokazao trgovac. Nakon toga odabire račun s kojeg će se skinuti određeni iznos i nakon što je odabrao račun terećenja, korisniku dolazi obavijest da je transakcija uspješno ili neuspješno obavljena [30].

M-zaba ja aplikacija Zagrebačke banke koja za svoje korisnike nudi puno mogućnosti kao što su otvaranje tekućeg i žiro računa, provjera stanja i prometa svih računa, kupnja bonova za mobitele, i još puno njih, ali među njima postoji i usluga IBAN QR kod kojom se mogu jednostavno prebacivati novčana sredstva drugim korisnicima m-zabe. Prije ulaska u aplikaciju korisnik mora unijeti PIN, nakon toga ulazi u opciju „Stanja i prometi“ gdje nakon toga odabire žiro ili tekući račun, odnosno račun koji će se teretiti. Nakon što je odabrao račun, korisnik odabire ikonu „IBAN[9] QR kod“ gdje ima dvije opcije: generiranje QR koda i učitavanje QR koda iz galerije kao što je prikazano na slici 4.12 [31].

[8] FIFO – metoda izlaska iz sustava na način „prvi ušao, prvi izašao“.

[9] IBAN – *„International Bank Account Number* je jedinstveni međunarodni identifikator računa klijenta u banci, određen u skladu s međunarodnim standardima Europske komisije za bankovne standarde ISO 13616“ [32].



Slika 4.12. Prikaz prozora „tekući račun“ i opcije IBAN QR kod, [31]

Ukoliko korisnik namjerava prebaciti sredstva na nečiji račun odabrat će opciju „Učitaj QR kod iz galerije“, nakon čega će se otvoriti kamera na mobilnom uređaju pomoću kojeg će korisnik učitati prethodno primljeni QR kod osobe kojoj vrši prijenos sredstava, te će korisnik potom unijeti iznos i potvrditi plaćanje. Ukoliko ipak korisnik očekuje uplatu od nekoga, podatke o IBAN-u svog računa može poslati u obliku QR koda izravno iz m-bankarstva odabirom opcije „Generiraj QR kod – Podijeli QR kod“ putem e-maila, Viber-a, društvenih mreža [31].

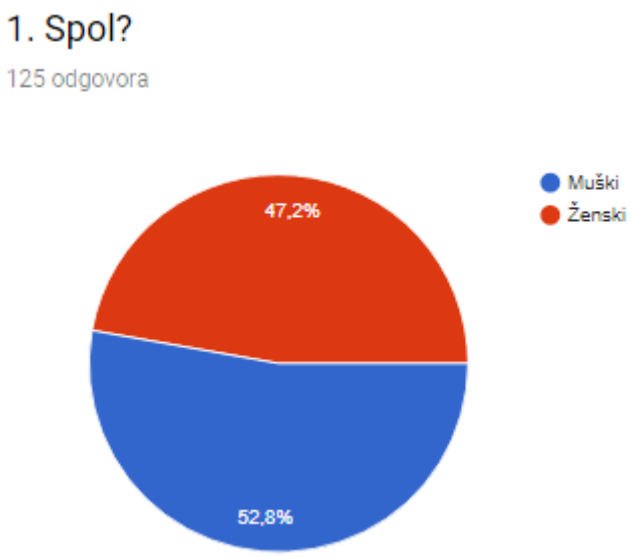
5 ANALIZA KORISNIČKOG ISKUSTVA PRI KORIŠTENJU USLUGA MOBILNOG ELEKTRONIČKOG POSLOVANJA

U ovome poglavlju opisati će se kakvo je korisničko iskustvo korištenja usluga mobilnog elektroničkog poslovanja. U tu svrhu provela se anketa u razdoblju od sedam dana (17.7. 2017. – 24.7.2017.) preko društvenih mreža (Facebook) i mobilnih aplikacija (*WhatsApp*). Istraživalo se kakva je trenutna razina korištenja usluga mobilnog elektroničkog poslovanja, kakva su iskustva korisnika, te koja je vrsta elektroničke naplate najzastupljenija. Kroz pitanja su se predložile i neke nove, ne toliko popularne tehnologije poslovanja (QR kodovi), te stavovi korisnika o novim tehnologijama, kao i njihovom prihvaćanju i korištenju u svakodnevnim situacijama.

Anketni upitnik sastojao se od 21 pitanja i ispunilo ga je 125 osoba. Prva 3 pitanja bila su demografske prirode (spol, broj godina i položaj u društvu), a zatim se prešlo na pitanja koja su vezana uz korištenje usluga mobilnog elektroničkog poslovanja. Pitanja su otkrivala kako korisnici najčešće plaćaju prilikom kupovine, odnosno u kojoj mjeri koriste elektronička plaćanja, te ukoliko ih koriste da navedu koja vrstu elektroničke naplate su koristili do sada, odnosno ako ne koriste da navedu jedan od ponuđenih razloga. Nadalje, pitanja su tražila općeniti dojam korisnika o elektroničkom plaćanju, te ih se pitalo jesu li čuli za „QR kodove“. Anketa je dalje istraživala koliko ih je koristilo „QR kodove“, u koje svrhe i gdje su se najčešće susretali sa njima. Zatim se od ispitanika tražilo da potvrde da li su čuli za bankarske usluge (aplikacije) koje također koriste „QR kodove“ kao tehnologiju naplate. Daljnja pitanja su bila napravljena da istraže u kojoj mjeri bi korisnici htjeli koristiti te usluge (aplikacije), te zbog kojih razloga, odnosno ukoliko ne bi htjeli, zbog kojih razloga ne. Zadnja četiri pitanja vezana su za sigurnosne prijetnje, provjeru učestalosti korištenja elektronskih naplata, ispitivanje korisnika u cilju saznavanja koji su to elementi njima bitni kod elektroničkih transakcija i na kraju u kolikoj mjeri su zadovoljni dostupnošću usluga mobilnog elektroničkog poslovanja u Republici Hrvatskoj.

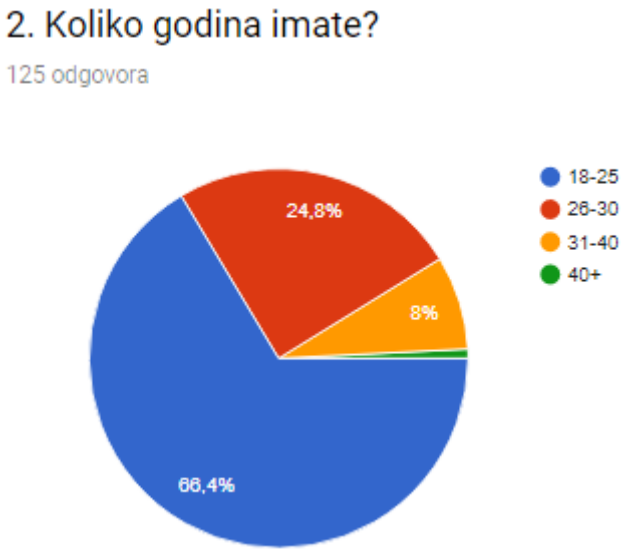
Na kraju diplomskog rada, u Prilogu 1., su anketna pitanja poredana po redu kako su bila i u stvarnoj anketi. Dalje u radu će se prikazati rezultati koji su dobiveni za svako pitanje u grafičkom obliku, kako bi bilo lakše shvatiljivo, i probat će se zaključiti nešto iz dobivenih rezultata.

Što se tiče spola od 125 ispitanih 59 se izjasnilo kao „ženski“, a 66 ispitanih kao „muški“, dok bi u postocima to bilo 47.2% ženskih osoba, odnosno 52.8% muških osoba kako je i prikazano na grafikonu 1 ispod.



Grafikon 5.1. Podjela prema spolu

Najveći broj ispitanika ima od 18 do 25 godina i njih ima 83, odnosno 66.4%, na drugo mjesto po brojnosti dolaze ispitanici u razmaku od 26 do 30 godina kojih ima 31, odnosno 24.8%. Druge dvije skupine ispitanika su puno manje i čine ih ispitanici od 31 do 40 godina kojih ima 10, odnosno 8% i samo jedan ispitanik koji se izjasnio da ima 40+ godina. Ispod na grafikonu 2 može se vidjeti grafički prikaz podjele po godinama.



Grafikon 5.2. Podjela prema godinama

Prema položaju u društvu, najveći broj ispitanika su studenti, i izjasnilo ih se 71 od 125 ukupno. To je zapravo i bio cilj, da se prikupe informacije od mlađih, školovanih generacija i da se vidi koliko oni zapravo koriste mobilno elektroničko poslovanje. Poslije studenata, tu su zaposleni ljudi kojih je u ovom ispitivanju bilo 46, dok je broj nezaposlenih bio 8. Umirovljenici nisu bili zabilježeni u ovoj anketi kao što je prikazano na grafikonu 3.

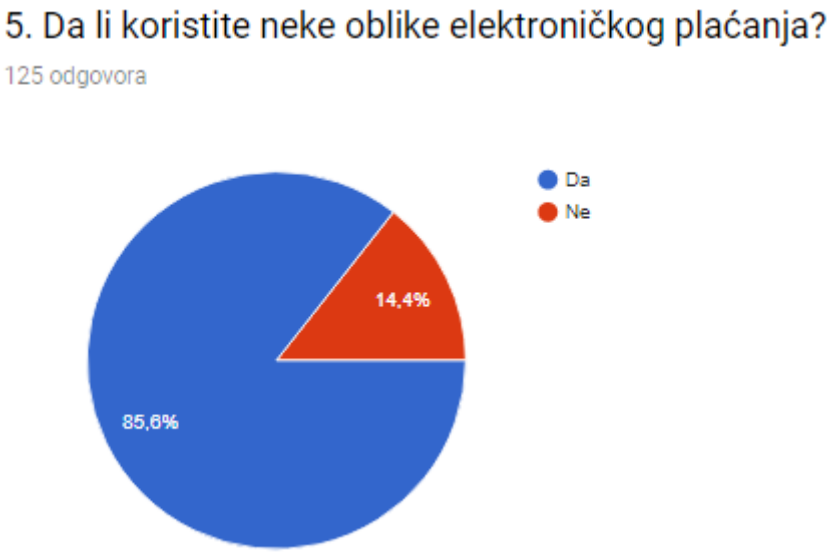
Grafikon 5.3. Podjela prema položaju u društvu

Najveći dio ispitanih najčešće plaća gotovinom, i to čak njih 82, zatim slijede ljudi koji plaćaju karticom i njih ima 41. Plaćanje mobitelom i internetom izgleda još

nije toliko popularno budući da su se samo 2 osobe izjasnile za te načine, za svaki po jedna kao što je prikazano na grafikonu 4.

Grafikon 5.4. Podjela prema najčešće korištenoj metodi plaćanja

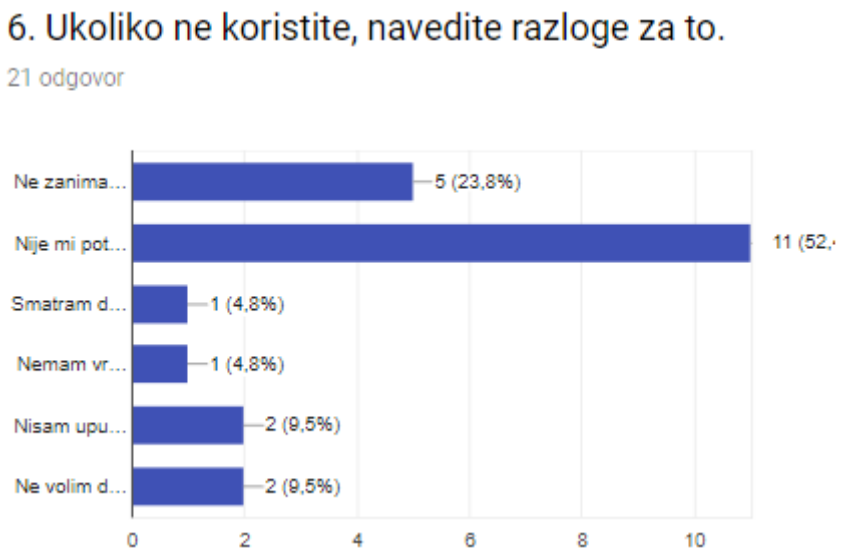
Na pitanje da li koriste neki oblik elektroničkog poslovanja od 125 ispitanih 107 ih je izjavilo „Da“, dok je njih 18 odgovorilo „Ne“ kao što je vidljivo na grafiokonu 5. Ispitanici koji ne koriste elektronička plaćanja morali su navesti razloge za to.



Grafikon 5.5. Podjela prema korištenju ili ne korištenju e-plaćanja

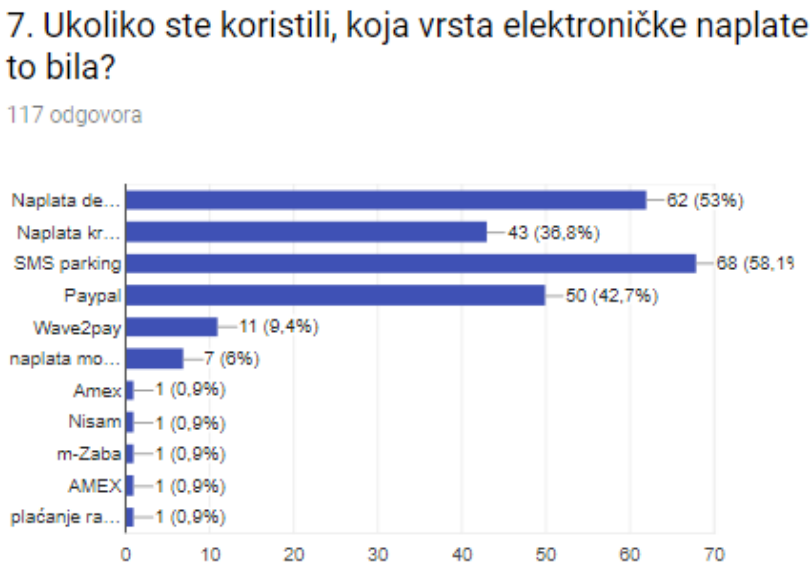
Prema anketi 5 puta je odabran razlog „Ne zanima me“ kao razlog ne korištenja, 11 puta „Nije mi potrebno“, jedanput „Smatram da mi je ugrožena sigurnost korištenjem e-plaćanja“ i „Nemam vremena“ za takav oblik plaćanja, 2 puta

„Nisam upućen u to“ i 2 puta „Ne volim davati osobne podatke nepoznatim sustavima“. Na grafikonu 6 vidi se kako to izgleda u postocima.



Grafikon 5.6. Razlozi zašto neki ispitanici ne koriste e-plaćanje

Ispitanici koji su se koristili elektroničkom naplatom izjavili su da su se najviše koristili SMS parkingom kao jednom vrstom elektroničke naplate i to njih 68. Nakon SMS parkinga, najviše korištene metode elektroničke naplate prema anketi su „Naplata debitnom karticom (Maestro)“ koju je odabralo 62 ispitanih, zatim „Paypal“ 50 ispitanih i „Naplata kreditnom karticom (MasterCard)“ 43 ispitanih. Nešto manje korištene metode elektroničke naplate u ovoj anketi bile su „Wave2pay“ koju je odabralo 11 ispitanih, zatim „Naplata mobilnim uređajem kroz razne „Wallet“ aplikacije (Google Wallet, Erste Wallet, Wallet)“ koju je odabralo 7 ispitanih, i pod rubrikom „Ostalo“ ispitanici su naveli (Amex, m-Zaba, korištenje mobilne aplikacije). Iz ovih rezultata vidljivo je da je većina ispitanih još uvijek više naklonjena kartičnom plaćanju nego naplati pomoću mobilnih aplikacija. Sve navedeno može se jednostavnije pogledati na grafikonu 7.



Grafikon 5.7. Vrste elektroničke naplate koje se koriste

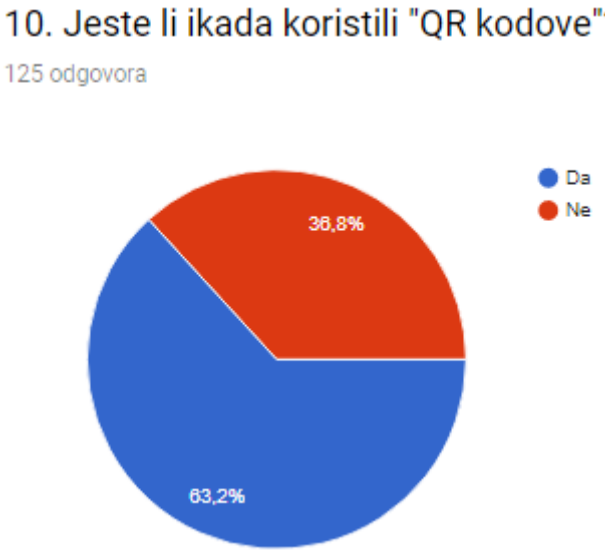
Na pitanje kakav je općeniti dojam o elektroničkom plaćanju 116 ispitanika je odgovorilo „Zadovoljan/na sam“, a „Nisam zadovoljan/na“ izjavilo je njih 9 od ukupno 125 ispitanih. Grafički prikaz vidljiv je na grafikonu 8.

Grafikon 5.8. Prikaz dojmova o elektroničkom poslovanju

Na pitanje jesu li čuli za „QR kodove“ čak 122 ispitanika su odgovorila sa „Da“, a samo njih 3 sa „Ne“ kao što je vidljivo na grafikonu 9. Ovo predstavlja dobar znak što se tiče daljnjeg razvoja sustava za plaćanje pomoću „QR kodova“ budući da je već veliki broj ljudi upoznat sa ovim oznakama.

Grafikon 5.9. Prikaz popularnosti „QR kodova“

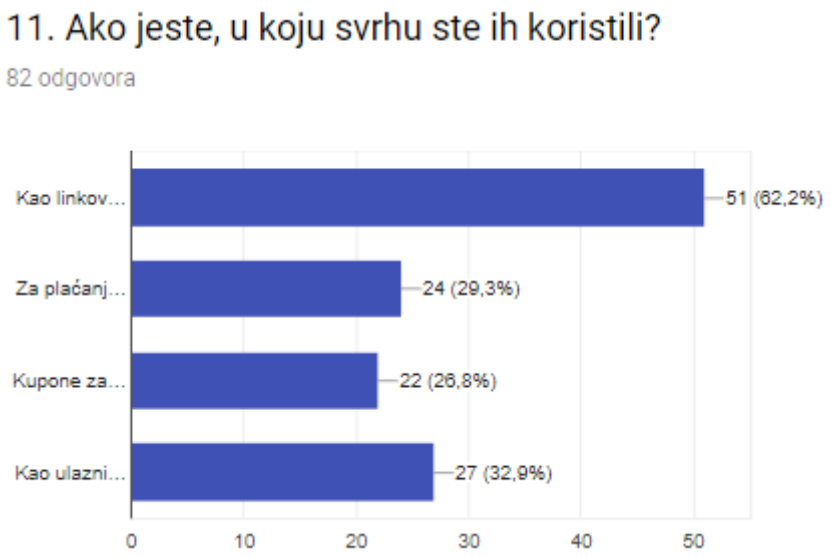
Na pitanje jesu li ikada koristili „QR kodove“ 79 ispitanika je izjavilo „Da“, a 46 njih reklo je „Ne“ kao što je vidljivo na grafikonu 10. Ovdje se vidi kako „QR kodovi“ još uvijek nisu toliko rašireni u svakodnevnom korištenju i da ih u tom smjeru ljudi još nisu dovoljno prihvatili.



Grafikon 5.10. Korištenje QR kodova

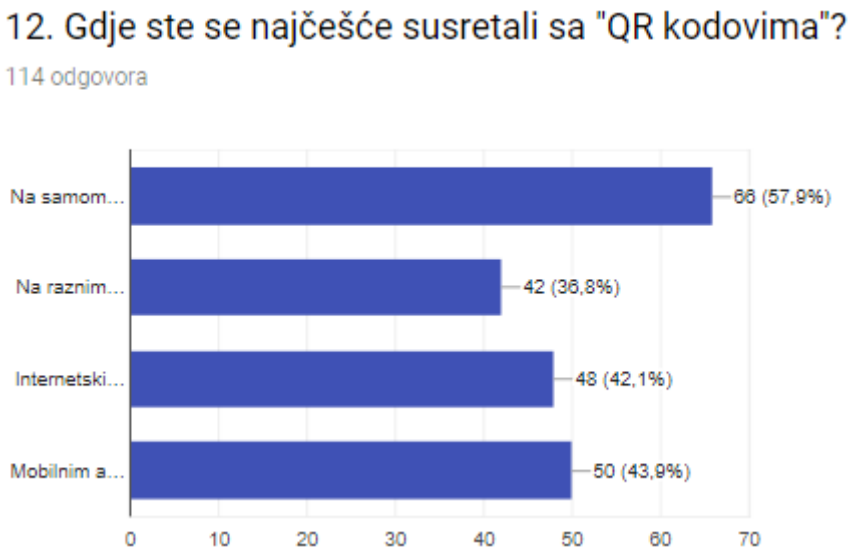
Na pitanje u koju svrhu su koristili „QR kodove“ odgovorilo je ukupno 82 ispitanika, odnosno oni koji su ih koristili. 51 ispitanik odgovorio je „Kao linkove za povezivanje na internetske stranice“, 27 njih reklo je da su ih koristili „Kao ulaznice za razne priredbe (kulturne,sportske)“, 24 njih odgovorilo je „Za plaćanje/prijenos novca“, 22 njih reklo je da ih je koristilo kao „Kupone za popuste“ kao što je vidljivo

na grafikonu 11. Ovih 24 ispitanika koji su „QR kodove“ koristili „Za plaćanje/prijenos novca“ dobar su znak da se „QR kodovi“ već dobrim dijelom koriste u mobilnom elektroničkom poslovanju. To je i znak se će se sigurno sve više koristiti i da treba obratiti pažnju na njih.



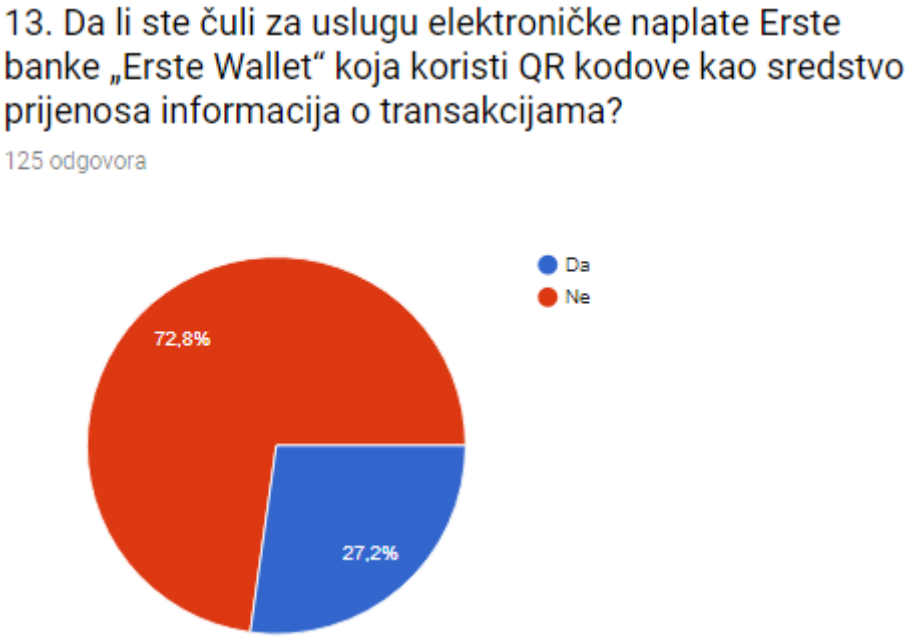
Grafikon 5.11. Prikaz svrhe korištenja „QR kodova“

Na pitanje višestrukog izbora, gdje su se najčešće susretali sa „QR kodovima“ 66 puta ispitanici su odabrali „Na samom proizvodu“, 50 puta na „Mobilnim aplikacijama“, 48 puta na „Internetskim stranicama“ i na kraju 42 puta „Na raznim plakatima po ulicama, trgovima“ kao što je prikazano na grafikonu 12. Iz ovih rezultata se vidi da ljudi primjećuju „QR kodove“ i prema tome ih treba što više koristiti u svakodnevnim aktivnostima, a onda postepeno i u specifičnim sustavima kao što su transakcije novca i razna plaćanja.



Grafikon 5.12. Prikaz učestalosti susreta sa „QR kodovima“ na specifičnim mjestima

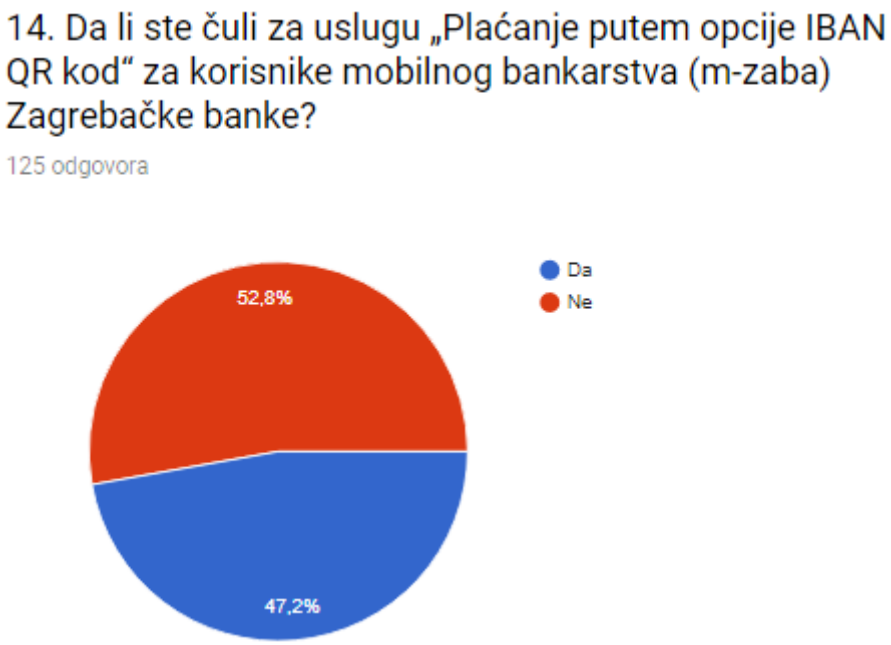
Kada je u anketi spomenuto da li su ispitanici čuli za uslugu elektroničke naplate Erste banke „Erste Wallet“ koja koristi „QR kodove“ kao sredstvo prijenosa informacija o novčanim transakcijama 91 osoba je rekla da nije čula, a samo 34 osobe su čule za tu uslugu kao što je prikazano na grafikonu 13.



Grafikon 5.13. Prikaz znanja ispitanika o novim uslugama Erste banke

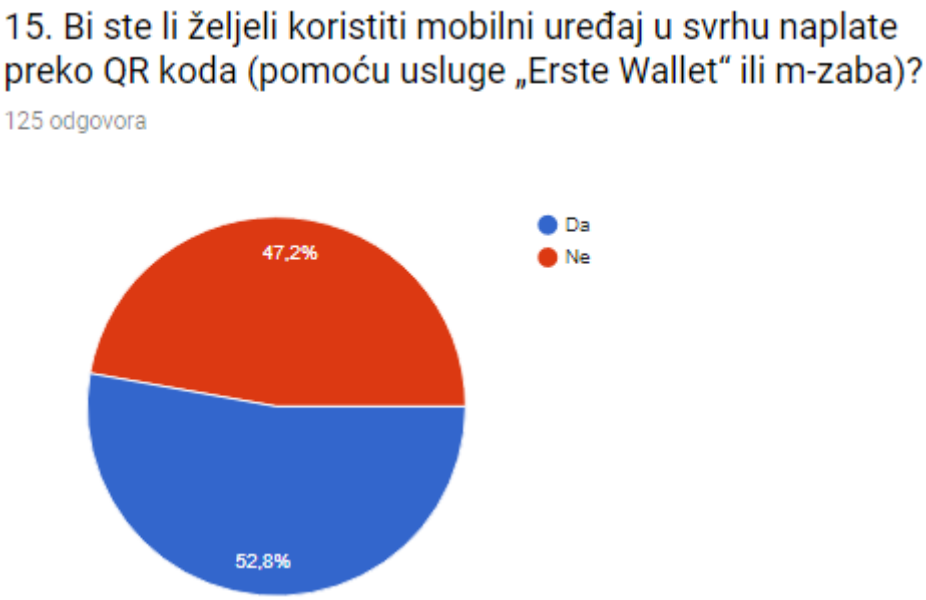
Malo bolje rezultate u smislu popuarnosti imala je usluga „Plaćanje putem opcije IBAN QR kod“ za korisnike mobilnog bankarstva (m-Zaba) Zagrebačke banke

za koju je čulo 59 ispitanika, odnosno 66 njih nije čulo. Kako to izgleda u postocima vidi se na grafikonu 14.



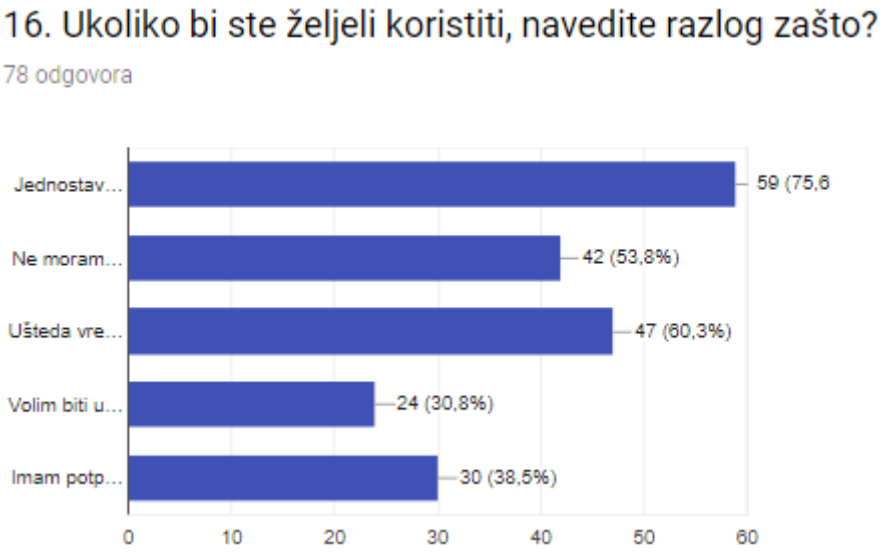
Grafikon 5.14. Prikaz znanja ispitanika o novim uslugama Zagrebačke banke

Na pitanje da li bi htjeli koristiti mobilni uređaj u svrhu naplate preko QR koda pomoću ranije spomenutih usluga „Erste Wallet“ i „m-Zaba“, 66 ispitanika odgovorilo je „Da“, dok je sa „Ne“ odgovorilo 59 ispitanika kao što se vidi na grafikonu 15. Ovi rezultati govore da su ljudi spremni prihvaćati i koristiti nove tehnologije, ali da one moraju biti prezentirane na pravi način, i da moraju funkcionirati bez greške.



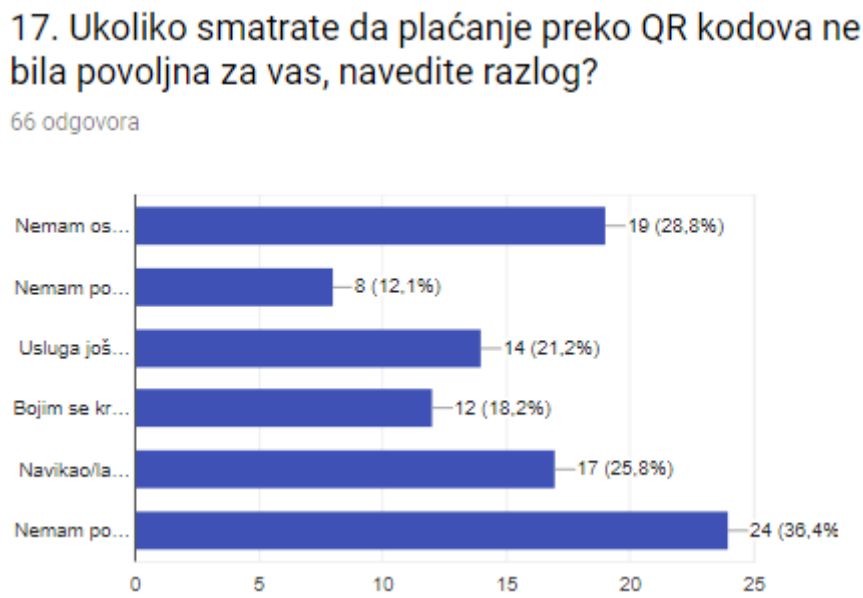
Grafikon 5.15. Grafički prikaz prihvaćanja i korištenja mobilnog uređaja kod ispitanika u svrhu naplate preko QR koda

Ispitanici koji su izjavili da bi htjeli koristiti mobilni uređaj u svrhu naplate preko QR koda, trebali su navesti razlog zbog kojeg bi to učinili. Najviše puta, čak 59, odabran je razlog „Jednostavna naplata“, zatim 47 puta „Ušteda vremena“, nakon toga 42 puta „Ne moram imati gotovinu kod sebe“, 30 puta „Imam potpuni pregled povijesti plaćanja, što kod gotovinskog plaćanja nemam“ i na kraju 24 puta „Volim biti u skladu s tehnologijom“ kao što je prikazano na grafikonu 16. Iz ovoga se da zaključiti da ljudi prepoznaju prednosti mobilnog elektronskog poslovanja i novih tehnologija i da ih prihvaćaju.



Grafikon 5.16. Razlozi prihvaćanja naplate preko QR koda

Nakon ispitanika koji su potvrdno odgovorili, ispitanici koji ne bi prihvatili plaćanje preko QR kodova morali su također odabrati razloge zbog kojih to ne bi učinili. 24 puta odabran je razlog „Nemam potrebu za time“, 19 puta „Nemam osjećaj koliko trošim“, 17 puta „Navikao/la sam isključivo na gotovinsko plaćanje“, 14 puta „Usluga još nije dovoljno zaštićena da bi ju koristio/la“, 12 puta „Bojim se krađe mobilnog uređaja i neovlaštenog korištenja“ i na kraju 8 puta „Nemam povjerenja u elektronsku naplatu“ kao što je prikazano na grafikonu 17. Iz rezultata se da zaključiti da još uvijek postoji dio ljudi koji ne prihvaćaju nove tehnologije i rješenja, te da su vjerni gotovinskom plaćanju. Istina je da i ova tehnologija ima negativne strane, međutim donosi puno više prednosti u odnosu na stari način plaćanja.

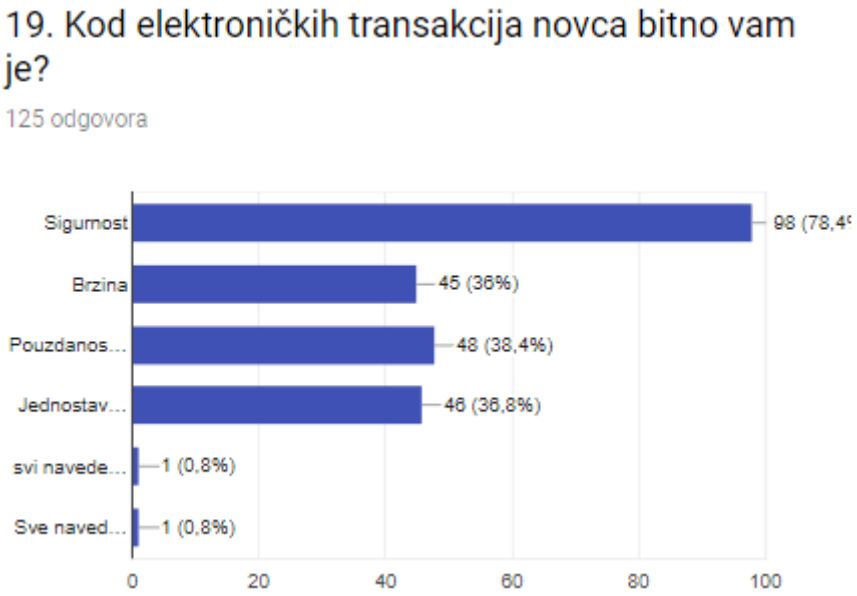


Grafikon 5.17. Razlozi ne prihvaćanja naplate preko QR kodova

Kada se govori o iskustvu sa sigurnosnim prijetnjama ili propustima pri elektroničkoj naplati ispitanici pokazuju različita iskustva. Najveći broj ispitanika, njih 79 izabrao je odgovor „Nisam imao takvih iskustva“. Nadalje, ispitanici koji su imali iskustva odabrali su sljedeće odgovore: 27 puta „Zastoj u radu aplikacije ili mobilnog uređaja“, 25 puta „Pucanje internetske veze prilikom naplate“, 10 puta „Nemogućnost očitavanja QR koda“, 6 puta „Krađa mobilnog uređaja“ i na kraju 5 puta „Hakerski napad“ kao što je i prikazano na grafikonu 18.

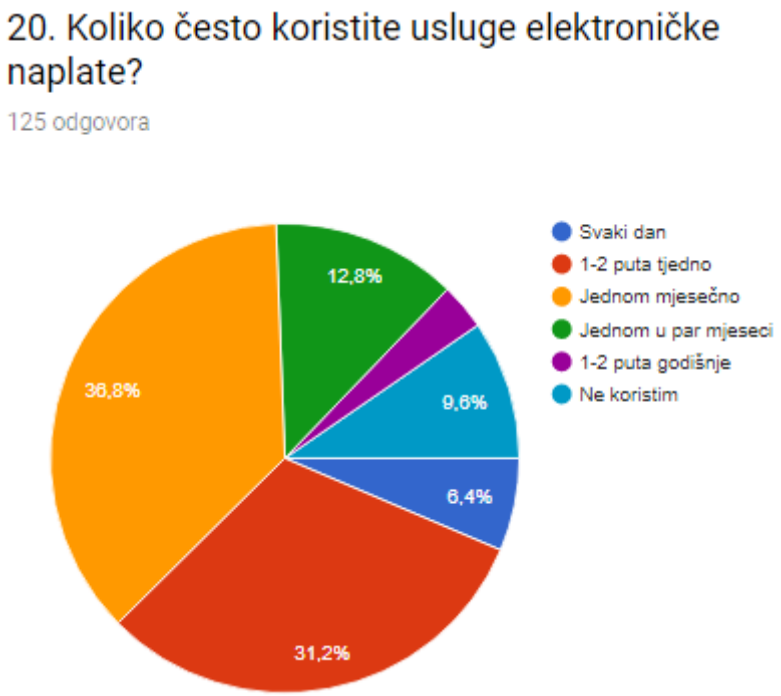
Grafikon 5.18. Iskustva sa sigurnosnim prijetnjama ili propustima

Na pitanje višestrukog izbora što je korisnicima elektroničkih transakcija bitno, čak 98 puta odabran je razlog „Sigurnost“, zatim 48 puta „Pouzdanost sustava“, 46 puta „Jednostavnost“, 45 puta „Brzina“ i dva ispitanika su odabrala „Sve navedeno“ kao što je prikazano na grafikonu 19. Iz ovih rezultata vidi se da je ispitanicima najvažnija sigurnost prilikom korištenja elektroničkih transakcija.



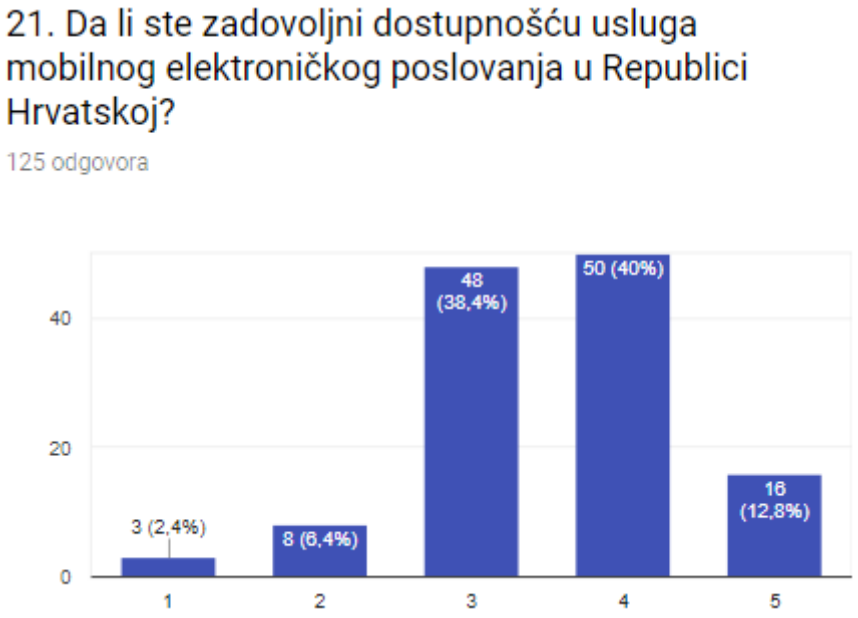
Grafikon 5.19. Izbor bitnih elemenata kod elektroničkih transakcija

Gotovo u svim ponuđenim odgovorima su se ispitanici podijelili što se tiče učestalosti korištenja usluga elektroničke naplate. Pa je tako zabilježeno 8 ispitanika sa odgovorom „Svaki dan“, 39 njih odgovorilo je „1-2 puta tjedno“, 46 ispitanika navelo je „Jednom mjesečno“, 16 njih „Jednom u par mjeseci“, 4 ispitanika „1-2 puta godišnje“ i na kraju ispitanici koji ne koriste ove usluge, njih je zabilježeno 12 kao što je i prikazano na grafikonu 20. Jako zanimljiv podatak je da 47 ispitanika koristi ove usluge barem jednom na dnevnoj, odnosno 1-2 puta na tjednoj bazi, što govori da je ovakav način plaćanja uvelike ušao u svakodnevnicu što je dobar znak za buduće tehnologije iz tog područja.



Grafikon 5.20. Grafički prikaz učestalosti korištenja usluga elektroničke naplate

I na kraju, na posljednje pitanje: „Da li ste zadovoljni dostupnošću usluga mobilnog elektroničkog poslovanja u Republici Hrvatskoj?“ dobiveni je jedan grafikon iz kojega se lijepo mogu vidjeti rezultati ankete. U pitanju je stavljena i skala (Nisam uopće zadovoljan(1) – U potpunosti sam zadovoljan(5)), koja dodatno objašnjava pitanje i ponuđene odgovore. Na grafikonu 21 mogu se pročitati rezultati ovog pitanja.



Grafikon 5.21. Zadovoljstvo dostupnošću usluga u RH

6 PRIJEDLOG ARHITEKTURE ZA MOBILNO PLAĆANJE POMOĆU QR KODA

Na osnovu prikupljenih podataka iz ankete o potrebama korisnika predlaže se arhitektura sustava za mobilno plaćanje primjenom QR koda. Predložena arhitektura trebala bi doprinijeti u sigurnosnom aspektu ove metode plaćanja, podići je na viši nivo i na taj način postati zanimljivija većem broju korisnika koji prema rezultatima ankete najviše zahtijevaju upravo sigurnost kod elektroničkih transakcija.

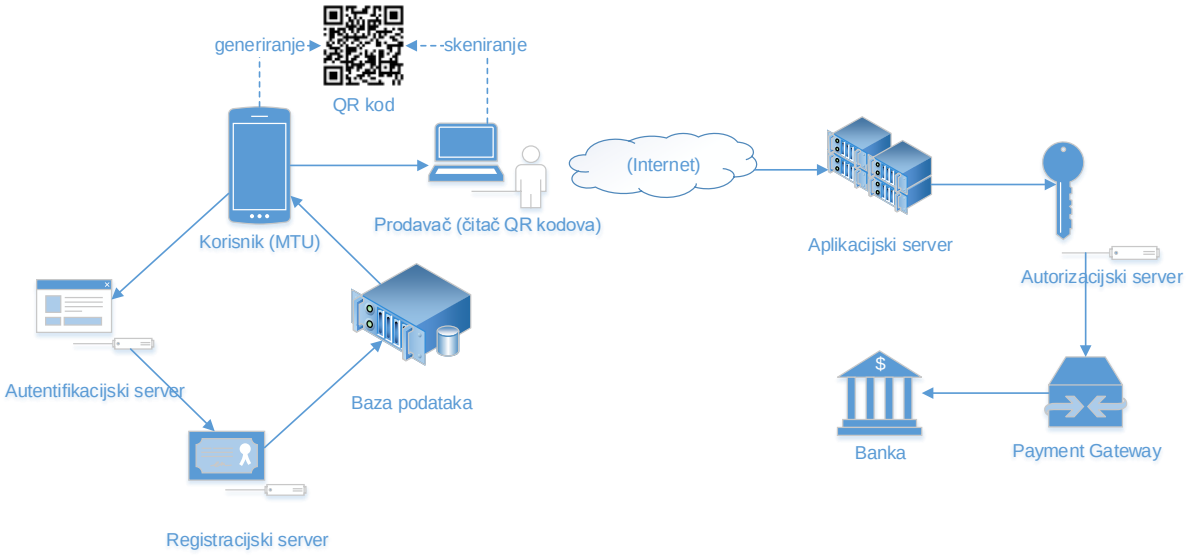
Osnovna svrha arhitekture nekog elektroničkog sustava je da na jednom mjestu prikaže sve bitne elemente tog sustava i način na koji su oni međusobno povezani. Arhitektura elektroničkog sustava obično se sastoji od: algoritama koji obrađuju podatke, spojeva između elemenata kojima se ostvaruje komunikacija, topologije koja opisuje kako su elementi organizirani.

Poznatiji stilovi u arhitekturi u računalstvu bili bi: slojevita arhitektura, arhitektura repozitorija podataka i arhitektura zasnovana na događajima. Slojevita arhitektura predstavljala bi organizaciju sustava u slojeve na način da se funkcionalnosti grupiraju po slojevima. Svaki sloj daje određenu uslugu sloju iznad i traži usluge od nižeg sloja, a najniži sloj sadrži jezgrene funkcionalnosti. Primjer jedne takve arhitekture bila bi telekomunikacijska mreža. Arhitektura repozitorija podataka opisana je na način da se upravljanje podacima vrši preko centralnog repositorija koji je dostupan svim komponentama sustava, s tim da su komponente nezavisne i ne moraju znati za postojanje ostalih komponenti u sustavu. Primjenjuje se kod velikih sustava koji koriste velike količine podataka koji se moraju pohraniti na neko vrijeme. Arhitektura zasnovana na događajima radi na principu difuznog emitiranja poruka. Izvori događaja (komponente) šalju poruke o tome da je nastupio neki događaj. Komponente koje objavljuju događaj nemaju informaciju koje će sve komponente reagirati i kako na taj događaj. Primjenjuje se u multiprocesorskim sustavima s više jezgara.

Arhitektura koja će se navesti za mobilno plaćanje pomoću QR kodova kombinacija je ovih stilova budući da postoji nekoliko slojeva unutar nje, radi se sa bazom podataka i određeni događaj pokreće cijeli proces. Navesti će se arhitektura, odnosno mogući scenarij kod plaćanja QR kodovima. Scenarij će se odnositi na

plaćanje korisnika koji koristi mobilnu aplikaciju povezanu sa kreditnim karticama, a sredstvo prijenosa informacija o transakciji biti će generirani QR kod.

Arhitektura bi se sastojala od sljedećih elemenata: korisnika, prodavača, aplikacijskog servera, autentifikacijskog servera, baze podataka, registracijskog servera, autorizacijskog servera, *Payment Gateway*-a i banke kao što je prikazano na slici 6.1.



Slika 6.1 Prijedlog arhitekture za mobilno plaćanje pomoću QR kodova

Korisnik uz pomoć mobilnog terminalnog uređaja (MTU) otvara instaliranu aplikaciju namjenjenu za plaćanje pomoću QR kodova. Korisnik pri ulasku u aplikaciju upisuje osobni PIN kako bi potvrdio svoj identitet na autentifikacijskom serveru i registrirao se. Nakon registracije baza podataka povlači sve podatke vezane uz korisnika (ime, prezime, adresa, kartice...), a korisnik odabire karticu kojom želi platiti uslugu ili proizvod. Nakon odabira kartice upisuje iznos, odnosno ukupnu sumu koju treba platiti, a koju je prodavač prethodno izračunao, i generira QR kod koji u sebi sadrži digitalni potpis kao dodatnu mjeru sigurnosti. U digitalnom potpisu sadržan je datum i vrijeme generiranja QR koda te iznos koji je plaćen. U QR kodu sadržani su podaci o vlasniku i vrsti kartice. Nakon što je QR kod izgeneriran, prodavač pomoć uređaja (čitača QR kodova) skenira taj isti kod. Podaci se odmah internetom šalju prvo na aplikacijski server budući da prodavač također koristi aplikaciju za cijeli proces, zatim se vrši autorizacija digitalnog potpisa da se provjeri da li je išta promjenjeno u odnosu na orginalni zapis. Tu se vrši i enkripcija podataka

iz generiranog QR koda, dakle prodavač niti u jednom trenutku ne saznaje podatke o karticama korisnika. Ukoliko je sve u redu preko *Payment Gateway*-a vrši se online autorizacija transakcije u realnom vremenu. Dakle *Payment Gateway* je softversko rješenje koje automatizira proces naplate između kupca, prodavača i banke. Proces naplate se odvija tako da *Payment Gateway* zaprima podatke (zapisane u generiranom QR kodu) s kreditnih kartica te ih prosljeđuje prema banci koja zatim autorizira ili odbija transakciju.

Najčešće korištene verzija QR koda kod ovakvih transakcija su verzije 25-30 budući da mogu pohraniti veću količinu podataka (podaci o kartici, korisniku, vremenu transakcije i digitalni potpis). Verzija 30 koja je prikazana na slici 6.2 može se pojaviti u 4 nivoa (L, M, Q, H) i dimenzija je 137x137 modula. Verzija 30 u svom alfanumeričkom zapisu u nivou L može pohraniti 2520 bit-a podataka.

Slika 6.2. Verzija 30 QR koda, [35]

Prednosti korištenja QR kodova pri plaćanju su brojne. Korisnik ove metode ne mora imati fizički novac uza sebe, dovoljno je da ima mobitel sa kamerom i instaliranom aplikacijom za plaćanje pomoću QR kodova. Plaćanje je jednostavno i brzo i omogućava pregled stanja prometa na računu i povijesti transakcija. Za trgovce ovakav način plaćanja je također prednost budući da banke ne uzimaju gotovo nikakav profit za transakcije te je jeftiniji i od gotovine kada se uzmu svi parametri u obzir. Što se tiče sigurnosnog aspekta, sigurnost je na vrlo visokoj razini, budući da se prije ulaska u aplikaciju mora unijeti osobni PIN, dakle i ukoliko osobi

nekim slučajem mobilni uređaj bude ukraden, počinitelj neće moći koristiti aplikaciju bez znanja osobnog PIN-a. Sigurnost pri plaćanju je isto na visokom nivou budući da bi se prema predloženoj arhitekturi koristio digitalni potpis koji osiguravao da nitko ne može presresti i promjeniti informacije koje se šalju prema prodavaču bez da se to kasnije ne može detektirati.

U nastavku će se navesti i neki nedostaci ove metode plaćanja, no njih nema puno. Kao prvo, ova metoda može se koristiti samo ako korisnik ima pristup internetu i mobilni uređaj sa kamerom na koji se može instalirati aplikacija. Nadalje, može se dogoditi da prilikom očitavanja generiranog QR koda dođe do greške i da se on ne može očitati, no to se događa vrlo rijetko.

7 ZAKLJUČAK

Usluge elektroničkog poslovanja pomogle su svijetu u njegovom razvoju, te se i same neprestano razvijaju i usavršavaju. Kako su to na početku bile jednostavne transakcije uz pomoć informacijsko-komunikacijske mreže koje nisu bile previše sigurne, razvijale su se sve brže i sigurnije metode. Tako su se pojavile nove metode koje su ljudi postepeno usvajali, a to su: kartično poslovanje, razni internet servisi za plaćanje (Paypal) koji nisu opisani u ovom diplomskom radu, te razna mobilna plaćanja (pomoću NFC tehnologije, SMS poruka, bluetooth tehnologije). Sve te metode pojavile su se kako bi olakšale i pojednostavile svakodnevna plaćanja i transakcije koje njihovi korisnici moraju obavljati. Kako bi se provjerilo koliko ljudi trenutno koristi određenu metodu napravljena je kratka anketa. U anketi je naglasak bio na QR kodovima, relativno novoj metodi plaćanja koja još nije dovoljno popularizirana i raširena, pa se htjelo vidjeti koliko ljudi znaju o ovoj tehnologiji i kako ju prihvaćaju.

Analizom prikupljenih rezultata ankete došlo se do zaključka da najveći dio ispitanika još uvijek najčešće koristi gotovinu kao platno sredstvo, ali odmah iza toga po postotku našle su se kartice, što pokazuje kako ljudi dosta koriste elektroničku naplatu. Najveći broj ispitanika usluge elektroničke naplate koristi jednom mjesečno, međutim postoje dvije manje skupine koje ih koriste 1-2 puta tjedno, odnosno druga skupina koja ih koristi na dnevnoj bazi, što pokazuje da je ovaj način plaćanja postaje svakodnevnica. Kao najčešće spomenut razlog ne korištenja elektroničkog plaćanja odabran je razlog „Nije mi potrebno“, što govori da određeni krug ljudi uopće ne želi koristiti taj oblik plaćanja dok postoji gotovina. Kod ispitanika koji su koristili elektroničku naplatu, kao što je i očekivano najčešće su odabirani odgovori: SMS parking, naplata debitnom karticom, naplata kreditnom karticom i paypal. Mali postotak, točnije 7 puta odabran je odgovor „Naplata mobilnim uređajem kroz razne „Wallet“ aplikacije (Google Wallet, Erste Wallet, Wallet)“ što pokazuje kako postoje korisnici i ovih metoda elektroničkog plaćanja i da ove metode imaju budućnost. Ispitanicima je kod elektroničkih transakcija novca najvažnija sigurnost, pa tek onda brzina, pouzdanost i jednostavnost kao što je vidljivo iz dobivenih rezultata. Ovo može biti smjernica pri dizajniranju novih ili usavršavanju postojećih metoda naplate, da se najviše pažnje posveti sigurnosti budući da je taj element prema rezultatima ankete korisnicima najbitniji. Kod iskustava sa sigurnosnim prijetnjama ili propustima

pri elektroničkoj naplati najveći broj ispitanika izjavio je kako nije imao takvih iskustava, međutim zabilježeni su i odgovori hakerskih napada, krađe mobitela, pucanja internetske veze, zastoja u radu aplikacije i nemogućnost očitavanja QR koda.

Dalje u anketi su se postavljala pitanja vezana uz QR kodove, pa je čak 97.6% ispitanika odgovorio kako je čuo za QR kodove, ali samo njih 63.2% ih je koristilo i to najčešće kao linkove za povezivanje na internetske stranice, a malo manji broj za plaćanje/prijenos novca. 27.2% ispitanika čuo je za uslugu elektroničke naplate Erste banke „Erste Wallet“ koja koristi QR kodove za prijenos novca. 47.2% njih je čuo za uslugu „Plaćanje putem opcije IBAN QR kod“ korisnika m-Zabe Zagrebačke banke. Postoci u prethodnim rečenicama nisu veliki, međutim čak 52,8% ispitanika izjavilo je kako bi željelo koristiti mobilni uređaj u svrhu naplate preko QR koda pomoću usluge „Erste Wallet“ ili usluge „plaćanje putem opcije IBAN QR kod“. Ovo pokazuje kako ljudi nisu dovoljno informirani o novim uslugama, jer prema ovima rezultatima pokazuju zanimanje za takve metode, ali jednostavno nisu čuli za njih pa ih niti ne koriste. Kao najveće razloge korištenja ovih metoda ispitanici navode jednostavnost naplate, ušteda vremena i to da ne moraju imati gotovinu kod sebe. Ispitanici imaju dobar dojam te su općenito zadovoljni elektroničkim plaćanjem, a zadovoljstvo dostupnošću usluga u Republici Hrvatskoj ocijenili su ocjenom vrlo dobar.

Prijedlog arhitekture za mobilna plaćanja pomoću QR kodova može donijeti na povećanju sigurnosnog aspetka u toj tehnologiji prijenosa informacija o transakcijama, budući da koristi digitalni potpis. Kao što je dobiveno iz rezultata ankete najveću važnost pri elektroničkim transakcijama korisnici posvećuju sigurnosti. Upravo digitalni potpis ubačen u generirani QR kod može donijeti na povećanju sigurnosti ove tehnologije i na taj način učiniti ovu metodu plaćanja globalnom.

LITERATURA

[1] URL: http://e-student.fpz.hr/Predmeti/S/Sustavi_elektronickog_poslovanja/Materijali/Klasifikacija_poslovanja.pdf (pristupljeno: travanj 2017.)

[2] URL: http://e-student.fpz.hr/Predmeti/S/Sigurnost_i_zastita_informacijsko_komunikacijskog_sustava/Materijali/P01_-_Elementi_informacijsko-komunikacijskog_sustava.pdf (pristupljeno: travanj 2017.)

[3] URL: http://repozitorij.fsb.hr/3062/1/Diplomski%20rad%20-%20Navijali%C4%87%20%281%29.pdf (pristupljeno: travanj 2017.)

[4] URL: https://poduzetnistvo.gov.hr/UserDocsImages/EU%20projekti/IPA%20IIIC/Pobolj%C5%A1anje%20poslovne%20konkurentnosti%20putem%20elektroni%C4%8Dkog%20poslovanja/13-e-poslovanje-handbook-hrweb.pdf (pristupljeno: svibanj 2017.)

[5] URL: http://e-student.fpz.hr/Predmeti/S/Sustavi_elektronickog_poslovanja/Materijali/6_Koncept_elektronicke_razmjene_podataka.pdf (pristupljeno: svibanj 2017.)

[6] URL: http://e-student.fpz.hr/Predmeti/S/Sustavi_elektronickog_poslovanja/Materijali/Sustavi_elektronickog_poslovanja_1.pdf (pristupljeno: svibanj 2017.)

[7] URL: http://sigurnost.zemris.fer.hr/en/2002_sipek/index.htm (pristupljeno: svibanj 2017.)

[8] URL: https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj97M6SxN7UAhVrEpoKHfl4DSYQFggjMAA&url=http%3A%2F%2Fwww.ss-zabok.skole.hr%2Fdokumenti%3Fdm_document_id%3D1186%26dm_rev%3D1%26dm_dnl%3D1&usg=AFQjCNEgixubApuSVQcBRbmBbF71XmW66g (pristupljeno: lipanj 2017.)

[9] URL: https://www.progreso.hr/blog/beskontaktno-placanje/ (pristupljeno: lipanj 2017.)

[10] URL: http://e-student.fpz.hr/Predmeti/S/Sustavi_pomocnih_tehnologija_u_prometu/Materijali/5_Razvoj_sustava_pomocnih_tehnologija_-_elementi_i_tehnologija.pdf (pristupljeno: lipanj 2017.)

[11] URL: http://www.ubs-asb.com/Portals/0/Casopis/2012/4/UBS-Bankarstvo-4-2012-Vaskovic.pdf (pristupljeno: lipanj 2017.)

[12] URL: http://searchcio.techtarget.com/definition/Google-Wallet (pristupljeno: lipanj 2017.)

[13] URL: https://www.techopedia.com/definition/27518/google-wallet (pristupljeno: lipanj 2017.)

[14] URL: http://android.appstorm.net/reviews/business-finance/google-wallet-makes-payments-truly-mobile/ (pristupljeno: srpanj 2017.)

[15] URL: http://www.smokvina.hr/hr/kategorije/opci-uvjeti/cvc (pristupljeno: srpanj 2017.)

[16] URL: http://mashable.com/2014/07/14/google-wallet-for-beginners/#.frEu8HiLGqw (pristupljeno: srpanj 2017.)

[17] URL: https://www.cnet.com/how-to/new-google-wallet-features-you-dont-want-to-miss/ (pristupljeno: srpanj 2017.)

[18] URL: https://randomoracle.wordpress.com/2014/06/14/coin-vs-google-wallet-comparing-card-aggregation-designs-part-ii/ (pristupljeno: srpanj 2017.)

[19] URL: https://arstechnica.com/gadgets/2014/10/how-mobile-payments-really-work/ (pristupljeno: srpanj 2017.)

[20] URL: http://www.kartice.ba/faq.php?type=poppit2-2sub1&page=1 (pristupljeno: srpanj 2017.)

[21] URL: https://www.hrvatskitelekom.hr/mobilne-usluge/usluge/sms/sms-parking (pristupljeno: srpanj 2017.)

[22] URL: http://blog.mahindracomviva.com/what-is-ble-mobile-payment/ (pristupljeno: srpanj 2017.)

[23] URL: https://www.google.hr/search?q=POS+beacon&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi5pMjh-LrUAhWFF5oKHYxWAiIQ_AUIBigB&biw=908&bih=662#tbm=isch&q=POS+beacon+types&imgrc=HIvyxmpTvk07UM: (pristupljeno: srpanj 2017.)

[24] URL: http://www.mbankcard.com/bluetooth-mobile-payments/ (pristupljeno: srpanj 2017.)

[25] URL: https://blog.beaconstac.com/2016/06/mobile-payment-showdown-android-pay-vs-apple-pay-vs-beacons/ (pristupljeno: srpanj 2017.)

[26] URL: https://www.adnovum.ch/en/company/focus/projects/twint_secure_payment_by_smartphone.html (pristupljeno: kolovoz 2017.)

[27] Ana Maria Cornelia, Elena Tirziman, Angela Repanovici, 2015. Stastical Research Regarding the Usefulness of Accessing Legal Information QR Coded; dostupno na linku: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=44c9d580-d4ca-4c9d-9d16-ff297f6defdb%40sessionmgr4009&vid=1&hid=4205 (pristupljeno: travanj 2017.)

[28] URL: http://www.qrcode.com/en/about/ (pristupljeno: kolovoz 2017.)

[29] Albăstroiu, I. and Felea, M., 2015. Enhancing the shopping experience through QR codes: the perspective of the Romanian users. Amfiteatru Economic, 17(39), pp. 553-566; dostupno na linku : http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=65ea5254-d73f-4db6-80e2-03560b9d8799%40sessionmgr4009&vid=0&hid=4205 (pristupljeno: travanj 2017.)

[30] URL: https://www.erstebank.hr/hr/gradjanstvo/e-bankarstvo/erste-wallet (pristupljeno: kolovoz 2017.)

[31] URL: file:///C:/Users/User/Downloads/uputa-za-koristenje-m-zabom1.pdf (pristupljeno: kolovoz 2017.)

[32] URL: https://www.pbz.hr/hr/iban (pristupljeno: kolovoz 2017.)

[33] URL: http://www.riteh.uniri.hr/zav_katd_sluz/zr/nastava/proginz/materijali/Dizajn%20programskog%20proizvoda.pdf (pristupljeno: kolovoz 2017.)

[34] URL: http://www.cert.hr/sites/default/files/NCERT-%20PUBDOC-2012-01-334.pdf (pristupljeno: kolovoz 2017.)

[35] URL: https://commons.wikimedia.org/wiki/File:Qr-code_2.jpg (pristupljeno: kolovoz 2017.)

POPIS ILUSTRACIJA

Popis slika

Popis grafikona

POPIS PRILOGA

Prilog 1. Anketni upitnik

U prilogu diplomskog rada nalazi se anketa, odnosno anketna pitanja. U anketi je bilo 21 pitanje. U zagradama se nalaze mogući odgovori:

1. **Spol?** (m/ž);
2. **Koliko godina imate?** (18-25, 25-30, 30-40, 40+);
3. **Položaj u društvu?** (Student/ica, Zaposlen/a, Nezaposlen/a, Umirovljen/a);
4. **Kako najčešće plaćate?** (Gotovinom, Karticom, Mobitelom, Internetom);
5. **Da li koristite neke oblike elektroničkog plaćanja?** (Da,Ne);
6. **Ukoliko ne koristite, navedite razloge za to.** (Ne zanima me, Nije mi potrebno, Smatram da mi je ugrožena sigurnost korištenjem e-plaćanja, Nemam vremena, Nisam upućen u to, Ne volim davati osobne podatke nepoznatim sustavima);
7. **Ukoliko ste koristili, koja vrsta elektroničke naplate je to bila?** (Naplata debitnom karticom (npr maestro), Naplata kreditnom karticom (npr. mastercard), SMS parking, Paypal, Wave2pay, razne „Wallet“ aplikacije (Google Wallet, Erste Wallet, Wallet), Ostalo);
8. **Kakav je vaš općeniti dojam o elektroničkom plaćanju?** (Zadovoljan/na sam, Nisam zadovoljan/na);
9. **Jeste li čuli za „QR kodove“?** (Da, Ne);
10. **Jeste li ikada koristili QR kodove?** (Da, Ne);
11. **Ako jeste, u koju svrhu ste ih koristili?** (Kao linkove za povezivanje na internetske stranice, Za plaćanja/prijenos novca, Kupone za popuste, Kao ulaznice za razne priredbe (kulturne, sportske..)
12. **Gdje ste se najčešće susretali sa „QR kodovima“?** (Na samom proizvodu, Na raznim plakatima po ulicama,trgovima; Internetskim stranicama, Mobilnim aplikacijama)
13. **Da li ste čuli za uslugu elektroničke naplate Erste banke „Erste Wallet“ koja koristi QR kodove kao sredstvo prijenosa informacija o transakcijama?** (Da, Ne);
14. **Da li ste čuli za uslugu „Plaćanje putem opcije IBAN QR kod“ za korisnike mobilnog bankarstva (m-zaba) Zagrebačke banke?** (Da, Ne);
15. **Bi ste li željeli koristiti mobilni uređaj u svrhu naplate preko QR koda (pomoću usluge „Erste Wallet“ ili m-zaba)?** (Da, Ne);

16. **Ukoliko bi ste željeli koristiti, navedite razlog zašto?** (Jednostavna naplata, Ne moram imati gotovinu kod sebe, Ušteda vremena, Volim biti u skladu s tehnologijom, Imam potpuni pregled povijesti plaćanja, što kod gotovinskog plaćanja nemam);
17. **Ukoliko smatrate da plaćanje preko QR kodova ne bi bila povoljna za vas, navedite razlog?** (Nemam osjećaj koliko trošim, Nemam povjerenja u elektronsku naplatu, Usluga još nije dovoljno sigurnosno zaštićena da bi ju koristio/la, Bojim se krađe mobilnog uređaja i neovlaštenog korištenja, Navikao/la sam isključivo na gotovinsko plaćanje, Nemam potrebu za time);
18. **Da li ste imali iskustva sa nekom od dolje navedenih sigurnosnih prijetnji ili propusta pri elektroničkoj naplati, izaberite jedan ili više odgovora?** (Hakerski napad, Krađa mobilnog uređaja, Pucanje internetske veze prilikom naplate, Zastoj u radu aplikacije ili mobilnog uređaja, Nemogućnost očitavanja QR koda, Nisam imao takvih iskustava)
19. **Kod elektroničkih transakcija novca bitno vam je?** (Sigurnost, Brzina, Pouzdanost sustava, Jednostavnost, Ostalo);
20. **Koliko često koristite usluge elektroničke naplate?** (Svaki dan, 1-2 puta tjedno, Jednom mjesečno, Jednom u par mjeseci, 1-2 puta godišnje, Ne koristim);
21. **Da li ste zadovoljni dostupnošću usluga mobilnog elektroničkog poslovanja u Republici Hrvatskoj?** (Nisam uopće zadovoljan(1) – U potpunosti sam zadovoljan(5));