UDC: 004. 621.39 Info M: str. 13-19

RAZVOJ USLUGE DIGITALNOG NOVČANIKA
DEVELOPING DIGITAL WALLET SERVICES

Dragana Vasiljević
Banca Intesa ad Beograd, dragana.vasiljevic@bancaintesa.rs
Prof. dr Zorica Bogdanović
Fakultet organizacionih nauka, Univerzitet u Beogradu, zorica@elab.rs
Aleksandra Vukmirović
Fakultet organizacionih nauka, Univerzitet u Beogradu, aleksandra.vukmirovic@stata.rs

REZIME: Predmet istraživanja ovog rada je razvoj rešenja mobilnog bankarstva korišćenjem bežičnih tehnologija. Rad ima za cilj da prikaže dizajniranje i implementaciju usluge Digitalnog novčanika koja će krajnjim korisnicima omogućiti vršenje mobilnih plaćanja neposrednim prinošenjem mobilnog telefona POS terminalima. Proces plaćanja se izvršava upotrebom virtuelne platne kartice na mobilnom telefonu korisnika korišćenjem HCE tehnologije. Razvijeno rešenje predstavlja primer inovativnog poslovnog modela kroz integraciju mobilnog i bankarskog poslovanja. Usluga Digitalnog novčanika, nazvana Wave2Pay, zasnovana je na NFC tehnologiji koja se koristi za beskontaktna plaćanja. Nova Wave2Pay usluga je novi metod plaćanja i trebalo bi da doprinese povećanju nivoa digitalizacije bankarskog sistema u Srbiji.

KLJUČNE REČI: bežične tehnologije, mobilna aplikacija, mobilno plaćanje, digital wallet, virtuelna kartica

ABSTRACT: The subject of this paper is the development of mobile banking solution using wireless technologies. The aim of this paper is to present the design and implementation of the Digital wallet service that will provide the end users with the option to make mobile payments by putting mobile phone near POS terminals. The payment process is executed with virtual payment cards on user's mobile phone using HCE technology. This developed solution is an example of a new business model through the integration of mobile and banking operations. The Digital Wallet service, named Wave2Pay, is based on the NFC technology which is used for contactless payments. The new Wave2Pay service is the new payment method that is likely to contribute in increasing the level of digitalization of the banking system in Serbia.

KEY WORDS: contactless technology, mobile application, mobile payment, digital wallet, virtual card

1. UVOD

Ubrzani tehnološki razvoj u posednjih nekoliko godina izazvao je konstantnu transformaciju poslovnih procesa, kao i pojavu inovativnih poslovnih modela u finansijama i bankarstvu. Prema istraživanju Republičkog zavoda za statistiku [1] 90,3% domaćinstava u Srbiji poseduje mobilni telefon. U nekim regionima sveta broj mobilnih telefona je u značajnoj meri nadmašio broj stanovnika. Značajan potencijal mobilnih plaćanja uslovio je zainteresovanost kompanija za povećanjem broja elektronskih transakcija dok brzina i dostupnost bankarskih transakcija sve više podstiču interesovanje krajnjih korisnika [2]. Mobilni telefon je postao potreba i uređaj bez koga je svakodnevni život nezamisliv. Sa ekspanzijom mobilnih telefona i potrebe korisnika se menjaju. Sem standardnih funkcionalnosti, korisnici sve više koriste mobilne telefone umesto kartica, ključeva, identifikacionih dokumenata, itd [3].

Korišćenjem NFC tehnologije omogućen je bežični prenos podataka koji nudi sigurnu, jednostavnu i intuitivnu komunikaciju između elektronskih uređaja. Korisnici uređaja sa NFC aplikacijama mogu jednostavno prisloniti svoj uređaj blizu drugog sličnog elementa koji podržava NFC tehnologiju u cilju komunikacije, čineći aplikaciju i korišćenje podataka jednostavnim i praktičnim [4].

U radu je dat prikaz analize razvoja i implementacije jednog inovativnog mobilnog servisa zasnovanog na NFC tehnologiji. Glavni cilj implementacije ovog projekta je razvoj Android aplikacije koja će ponuditi korisnicima novi način mobilnih plaćanja neposrednim prinošenjem telefona POS terminalima.

2 ANALIZA LITERATURE

2.1 *NFC tehnologija*

NFC (Near Field Communication) je vrsta tehnologije koja predstavlja integraciju RFID (Radio Frequency Identification) tehnologije sa mobilnim uređajima [6]. Ona omogućava komunikaciju jednostavnim dodirivanjem ili prinošenjem dva uređaja u neposrednu blizinu [5]. RFID se uglavnom koristi kod aplikacija za identifikaciju proizvoda ili osoba bez optičke vidljivosti. NFC se sa druge strane koristi za sofisticirane i sigurne transakcije kao što je beskontaktni pristup ili plaćanje. NFC tehnologija je već ugrađena u mnoge smart telefone, ali se još uvek nedovoljno koristi [7].

Postoje mnoge tehnologije koje su slične NFC tehnologiji po svojim karakteristikama, kao što je RFID (Radio-frequency identification), IrDA (Infrared Data Association Protocol) i Bluetooth. Svaka od njih poseduje određene prednosti i nedostatke u odnosu na druge. U tabeli je dat uporedni prikaz ovih tehnologija [8].

	NFC	RFID	IrDA	Bluetooth
Vreme uspostavljanja konekcije	<0.1 ms	<0.1 ms	~0.5 s	~6 s
Domet	do 10 cm	do 3 m	do 5 m	do 30 m
Korišćenje	orijentisan na čoveka, jednostavan, intuitivan, brz	objektno orijentisan	orijentisan na podatke	orijentisan na podatke
Upotreba	plaćanje, pristup podacima, razmena podataka	praćenje predmeta	kontrola i razmena podataka	razmena podataka
Iskustva potrošača	jednostavno povezivanje (dodir, mahanje)	preuzimanje informacija	jednostavan za upotrebu	sistemski zahtevi

Tabela 1. Uporedni prikaz beskontaktnih tehnologija [9]

NFC predstavlja tehnologiju kratkog dometa koja koristi indukciju magnetnog polja kako bi omogućila komunikaciju između dva uređaja koja se nalaze na neposrednoj udaljenosti od nekoliko centimetara [10]. Za komunikaciju preko NFC tehnologije, neophodno je da jedan uređaj bude čitač/pisač, a drugi NFC tag [11]. Tag predstavlja integrisano polje koje sadrži podatke koji mogu biti napisani ili pročitani sa čitača. NFC je dizajniran tako da jedan uređaj u jednom trenutku može da se koristi za slanje ili za prijem podataka. Preciznije rečeno, dok jedna strana šalje podatke, druga osluškuje. Postoje tri tipa uređaja koja se mogu koristiti za transfer podataka preko NFC tehnologije:

- NFC čitač – inicijator NFC komunikacije;
- NFC mobilni telefon – aktivni i pasivni uređaj, u zavisnosti od potreba aplikacije u kojoj se koristi;
- NFC tag – pasivni uređaj koji komunicira sa aktivnim uređajem.

U zavisnosti od načina na koji se prenose podaci između aktivnih i pasivnih uređaja, razvijena su tri moda funkcionisanja [12]:

1) Peer-to-peer mod – Ovaj model podržava direktnu razmenu informacija između dva aktivna NFC čipa. Uređaji funkcionišu tako da jedan uređaj inicira transakciju dok drugi uređaj odgovara na zahtev. Dobar primer ovog moda je razmena sadržaja (video zapisi, muzika, kontaktne informacije) dodirivanjem dva mobilna telefona.
2) Mod čitanja/pisanja - Ovaj mod dozvoljava inicijatoru da čita sa ili piše na drugi NFC tag. Primer korišćenja ovog moda bi mogla biti situacija kada korisnik približi svoj NFC telefon određenom predmetu i tom prilikom dobije informacije koje su za njega značajne, kao što su opis proizvoda, tehnička specifikacija, cena, specijalne ponude, marketinške promocije, demo prikazi, komentari ili preporuke osoba koje ga već koriste, i slično.
3) Mod imitiranja kartice – ovaj mod se uglavnom koristi kao podrška mobilnom plaćanju, ali se takođe koristi i za simulaciju različitih kartica (kartice lojalnosti, medicinske kartice, članske karte, sezonske karte, itd) [13].

NFC tehnologija ima nekoliko prednosti u odnosu na druge bežične tehnologije jer obezbeđuje dvosmernu komunikaciju za razmenu informacija, tj. oba uređaja mogu primiti ili poslati podatke istovremeno, za razliku od Bluetooth-a koji karakteriše jednosmerna komunikacija. Još jedna prednost NFC-a je ta što troši manje energije u odnosu na Bluetooth [14]. Manje baterije se koristi pošto je za NFC tehnologiju karakteristična manja brzina prenosa od 106 kbps do 424 kbps [15].

Sa većom popularnošću Android operativnog sistema, upotreba sistema zasnovanih na NFC tehnologiji postaje rasprostranjenija i više se koristi u svrhu plaćanja. Veliki broj platnih sistema zasnovanih na NFC tehnologiji razvijen je od 2003. godine. Mnogi od njih su ubrzo i ugašeni. Razlog tome je mali broj mobilnih telefona koji su u to vreme podržavali NFC tehnologiju. Trenutna situacija na tržištu mobilnih telefona je takva da njihov broj značajno raste u poslednjih nekoliko godina. Plaćanja korišćenjem mobilnih telefona zasnovanih na NFC tehnologiji mogu biti izvršena na POS terminalima. Plaćanje se izvršava tako što se mobilni telefon prinese blizu beskontaktnog POS terminala. Proces plaćanja se izvršava upotrebom virtuelne platne kartice na mobilnom telefonu korisnika.

2.2 *HCE*

Sa uvođenjem HCE (Host Card Emulation) omogućeno je funkcionisanje aplikacija zasnovanih na NFC tehnologiji bez neophodnog prisustva kartice. Platna aplikacija je ugrađena u operativni sistem mobilnog telefona (“host”). HCE omogućava bankama da pokrenu NFC proizvod na mobilnom telefonu bez potrebe za korišćenjem SIM-a ili drugog sigurnog elementa [16], dozvoljavajući operativnom sistemu mobilnog uređaja direktnu komunikaciju preko NFC interfejsa u modu imitiranja kartice . HCE tehnologija omogućava da se platna aplikacija nalazi u operativnom sistemu mobilnog telefona i da ona komunicira direktno sa NFC antenom [17].

HCE je softver dizajniran tako da omogući tačan virtuelni prikaz različitih elektronskih identifikacionih (pristupnih, tranzitnih ili platnih) kartica korišćenjem isključivo softvera. HCE omogućava pokretanje mobilnih aplikacija na podržanim operativnim sistemima sa funkcionalnošću platnih kartica [18]. Ova tehnologija podržava pristup rešenjima nezavisno od treće strane uz usklađivanje kriptografskih procesa koji se konvencionalno koriste od strane hardverski zasnovanih sigurnosnih elemenata bez potrebe za fizičkim prisustvom sigurnosnih elemenata. Mobilno plaćanje se tradicionalno čuvalo lokalno na mobilnom uređaju u delu hardvera koji se zove sigurnosni element (Secure element) [19]. HCE tehnologija oponaša platne kartice na mobilnom uređaju koristeći samo softver. Kroz mobilni operativni sistem omogućava da „virtuelni” sigurnosni element bude prisutan van mobilnog uređaja [20]. Pomeranjem ovog elementa na izmeštenu lokaciju, tehnikalije i prate-

ći troškovi se mogu zanemariti. Proizvođači aplikacija mogu direktno razviti svoje aplikacije bez uključivanja posrednika [21].

HCE otvara razne mogućnosti za razvoj različitih rešenja. Ovo stvara mogućnost za servis provajdere da na jednostavan način i sa uspehom implementiraju NFC usluge [22] i na taj način omogućavaju ostvarivanje finansijskih ciljeva, industrijskih mogućnosti i bezbednosnih zahteva [223].

3 DIZAJN I IMPLEMENTACIJA REŠENJA

3.1 *Specifikacija korisničkog zahteva*

Na osnovu rezultata dobijenih instraživanjem tržišta, Banca Intesa je u saradnji sa Intesa Sanpaolo Card (ISPC) razvila novo rešenja mobilnog poslovanja. Ovim rešenjem će u narednom periodu biti omogućeno korišćenje virtuelne kartice u Digitalnom novčaniku korisnika. Svaki klijent koji aplicira za Digitalni novčanik i virtuelnu karticu biće u mogućnosti da plaća na POS terminalima bez korišćenja kartice u plastici.

Korisnički zahtev je obuhvatao plaćanja zasnovana na HCE (Host Card Emulation) tehnologiji virtualizovanjem platne kartice u cloud, čime se omogućava plaćanje preko smart telefona. Usluga će u startu biti omogućena korisnicima koji poseduju smart telefone zasnovane na Android operativnom sistemu sa NFC mogućnostima i verzijom 4.4 (KitKat) operativnog sistema ili novijim. HCE usluga bi se realizovala u okviru aplikacije mobilnog novčanika za unapred definisane platne kartice uz korišćenje tokenizacije.

Virtuelna kartica će biti skladištena u cloud-u i korisnik će pristupanjem svom Digitalnom novčaniku koji je preuzeo sa Google Play prodavnice preuzeti kredencijale za plaćanje na svoj smart telefon. Važno je naglasiti da je korišćenje virtuelne kartice i vršenje plaćanja moguće samo kroz Digitalni novčanik. Ova aplikacija je zaštićena odgovarajućim kodom koji je potrebno uneti svaki put kada se aplikacija koristi. Kroz aplikaciju Digitalnog novčanika korisnik će biti u mogućnosti da prati stanje po računu, kao i spisak transakcija izvršenih virtuelnom karticom.

Za korišćenje određenih funkcionalnosti neophodno je da mobilni telefon ima pristup internetu. Detalji sa kartice, kao i kredencijali plaćanja, se ne čuvaju unutar digitalnog novčanika i preuzimaju se svaki put kada korisnik otvori aplikaciju [24].

3.2 *Bezbednosni aspekt*

Prilikom implementacije novog modela mobilnog plaćanja važno je obezbediti visok nivo sigurnosti. Kao prva mera bezbednosti može se navesti mogućnost zaključavanja smart telefona tako da niko drugi ne može da ga koristi bez autorizacije. Kada korisnik prvi put startuje Wave2Pay aplikaciju, korisnik mora da ukuca passcode koji se sastoji od četiri cifre. Sledeći element je postojanje sigurnosnog čipa [25] koji čuva šifrovane poverljive podatke o korisniku. Čipu mogu pristupiti samo autorizovani programi. Sa sigurnosnog aspekta, vrlo je važno uzeti u obzir i to da je prosečnom korisniku kartice potrebno duže da shvati da je izgubio karticu nego mobilni telefon. Kada se kartice nalaze u telefonu, bezbednost je povećana pošto će korisniku svakako biti potrebno manje vremena da primeti da mu je telefon ukraden. Na taj način korisnik će imati mogućnost da brzo reaguje i spreči pojavu potencijalno neželjenih posledica.

Tokom procesa aktivacije usluge Digitalnog novčanika, iz bezbednosnih razloga, klient dobija dva kredencijala koja su neophodna za aktivaciju usluge (Aktivacioni kod i Aktivacini ključ). Ovi kredencijali se dostavljaju korišćenjem različitih kanala za distribuciju. Banka će generisati Aktivacioni ključ i dostaviti ga korisniku odštampanog u zatvorenoj PIN koverti. Aktivacioni ključ je jedinstven za korisnika i predstavlja statički podatak. Drugi parametar (Aktivacioni kod) generiše Procesor (ISPC) i dostavlja ga korisniku putem SMS-a. Neophodno je da ovaj kod bude dinamički, tj. da prilikom svakog novog korišćenja ima drugu vrednost.

Nakon što je usluga aktivirana klijent preuzima aplikaciju Digitalnog novčanika (Wave2Pay) sa Google Play prodavnice. Kako bi aktivirao aplikaciju klijent će morati da ukuca Aktivacioni ključ i broj svog mobilnog telefona. Na serveru će biti provereno da li je otvoren nalog za određenog klijenta kao i broj mobilnog telefona klijenta. Ukoliko je ishod pozitivan, jednokratni Aktivacioni kod će se generisati od strane servera i biće poslat SMS na mobilni uređaj klijenta. Kada klijent primi SMS na svom mobilnom telefonu sa Aktivacionim kodom, aplikacija Digitalnog novčanika je automatski aktivirana. Tokom aktivacije aplikacije korisnik će biti navođen kroz aplikaciju kako bi definisao lozinku (mPIN) za pristup mobilnoj aplikaciji i za autorizovanje transakcija. Server aplikacije pribavlja podatke o kartici za svakog klijenta pojedinačno iz back office aplikacije i upisuje ga u nalogu Digitalnog novčanika korisnika. Prilikom svakog pristupa aplikaciji Digitalnog novčanika ili prilikom autorizacije transakcije u procesu plaćanja neophodno je da korisnik unese mPIN.

Prilikom implementacije Digitalnog novčanika kao jedan od načina zaštite osetljivih podataka korišćen je postupak tokenizacije. Tokenizacija je proces zamene osetljivih podataka neosetljivim podacima koji nemaju upotrebnu vrednost. Token je identifikator koji predstavlja pokazatelj na osetljive podatke kroz sistem za tokenizaciju. Mapiranje originalnih podataka tokenima koristi metode koje čine tokene neupotrebljivim u odsustvu sistema za tokenizaciju. Sistem za tokenizaciju obezbeđuje prava i interfejs za obradu podataka u aplikaciji kako bi se dobio token, ili povratni proces detokenizacije kako bi se dobili osetljivi podaci.

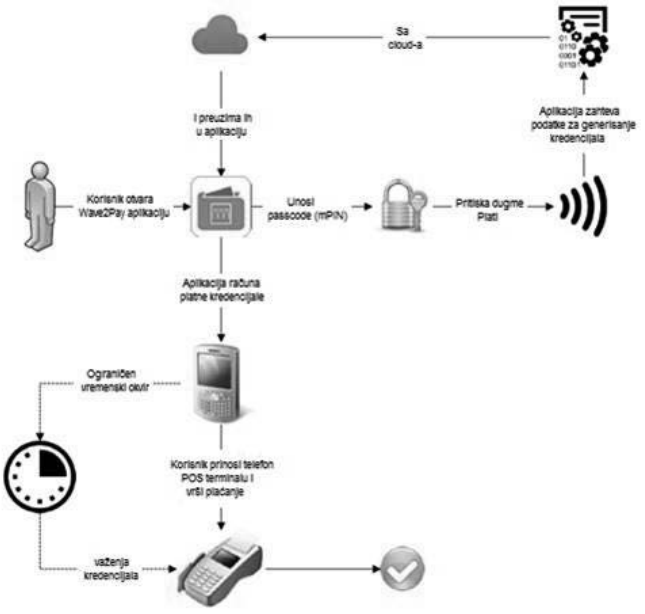
Prednosti tokenizacije kao što su bezbednost i smanjenje rizika zahtevaju da je sistem za tokenizaciju lokalno izolovan i segmentiran od sistema za obradu podataka i aplikacija koje su prethodno obradile i sačuvale osetljive podatke zamenjene tokenima. Samo sistem za tokenizaciju može tokenizovati podatke i kreirati tokene, ili detokenizovati nazad u osetljive podatke pod strogim sigurnosnim kontrolama. Metod za generisanje tokena mora biti takav da ne sme dozvoliti ni na koji način, bilo kojom vrstom direktnih napada, kriptoanalize ili drugih tehnika da se dođe do „živih" podataka.

Kada tokeni zamene prave podatke u sistemu, rezultat je minimalno izlaganje osetljivih podataka ovoj aplikaciji, prodav-

nici gde je aplikacija izložena, ljudima i procesima, redukujući pri tom rizik od slučajnog izlaganja i neautorizovanog pristupa osetljivim podacima. Aplikacija može da funkcioniše korišćenjem tokena umesto živim podacima, sa izuzetkom malog broja poverljivih aplikacija sa eksplicitnom dozvolom za detokenizaciju kada je to neophodno za odobrene poslovne svrhe [26].

3.3 *Tok procesa*

Za uslugu digitalnog novčanika, klijent (pojedinac) može da aplicira u bilo kojoj ekspozituri Banke. Za mobilna plaćanja, u okviru digitalnog novčanika, neophodno je da klijent zahteva virtuelnu karticu iz ponude Banke, namenjenu beskontaktnom plaćanju. Prilikom aktivacije usluge digitalnog novčanika u ekspozituri, neophodno je klijentu generisati jedinstveni Aktivacioni ključ (slika 1). U isto vreme klijent dobija i Aktivacioni kod. U momentu kada je nalog za Digitalni novčanik za specifičnog klijenta otvoren, broj mobilnog telefona je obavezan podatak [27].

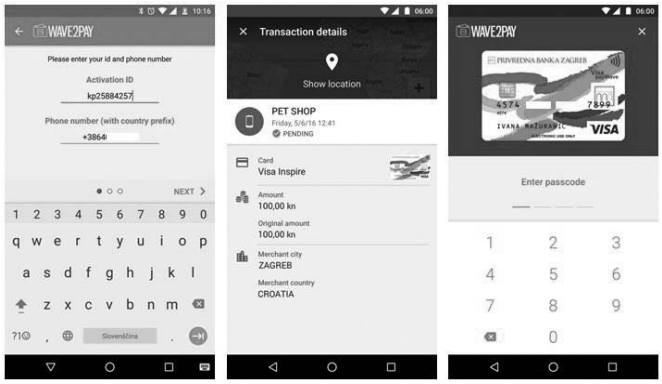


Slika 1. *Tok procesa [28]*

Virtuelna platna kartica će biti ponuđena kao novi proizvod u Banci, korišćenjem podopsega postojećih BIN-ova platnih kartica. Virtuelna kartica će imati iste parametre kao i fizički proizvod osim što će korišćenje biti ograničeno. Važenje virtuelne kartice će pratiti postavke fizičke kartice. Predviđeno je da se virtuelne kartice koriste samo na beskontaktnim POS terminalima. Za ovaj tip proizvoda, PIN koji je zajednički za korišćenje kod plastične kartice i koji se unosi na POS terminalima i na bankomatima, se ne koristi i neće biti generisan.

Virtuelna kartica će biti podešena tako da fukcioniše online i sve transakcije će zahtevati online potvrdu. Korišćenje virtuelne kartice će biti moguće za transakcije koje se izvrše na bežičnim POS terminalima. Ovaj vid kartica može biti korišćen za domaća i inostrana plaćanja. Ostale transakcije kao što su e-commerce, MO-TO, POS cash, kao i podizanje gotovine na bankomatima korišćenjem virtuelnih kartica u prvoj fazi neće biti moguće.

Svaki put kada korisnik otvori aplikaciju Digitalni novčanik, podaci o kartici će biti sinhronizovani sa back office aplikacijom. Podaci koji se sinhronizuju su: ime klijenta, ime koje je utisnuto na kartici, broj mobilnog telefona korisnika, status kartice, blokada kartice, itd.



Slika 2. *Usluga Digitalnog novčanika [29]*

Na slici 2 je dat prikaz kartice u aplikaciji Digitalnog novčanika, embosirano ime korisnika, kao i datum isteka kartice. Klijent je u mogućnosti da promeni te podatke u mobilnoj aplikaciji, ali promena ovih podataka neće uticati na performanse kartice. Ukoliko se promeni status kartice u back office aplikaciji, kada je kartica deaktivirana, kartica će biti uklonjena iz Digitalnog novčanika i neće biti vidljiva za klijenta. Klijent će takođe dobiti SMS notifikaciju o ovom događaju. Situacija je identična i u slučaju blokade kartice.

Svaki klijent može da ima instaliranu aplikaciju Digitalnog novčanika isključivo na svom mobilnom uređaju. Aktivacija aplikacije na novom uređaju će automatski deaktivirati i onemogućiti korišćenje na starom uređaju. Kako bi aktivirao aplikaciju na novom uređaju neophodno je da klijent unese Aktivacioni ključ i broj mobilnog telefona, a procesor će poslati klijentu SMS sa Aktivacionim kodom.

U slučaju kada korisnik izgubi svoj mobilni telefon, dužan je da to prijavi Banci. U toj situaciji svi uređaji klijenta će biti uklonjeni iz njegovog naloga. Biće kreiran novi Aktivacioni kod. Aplikacija Digitalnog novčanika na izgubljenom ili ukradenom mobilnom uređaju neće više biti upotrebljiva, a dalja aktivacija aplikacije upotrebom starog Aktivacionog koda neće biti moguća. Kada klijent želi da instalira aplikaciju na novom mobilnom uređaju, potrebno je da se obrati Banci. Tom prilikom će mu biti generisan Aktivacioni kod i biće inicirana procedura redistribucije.

U aplikaciji Digitalnog novčanika omogućeno je korišćenje mPIN-a za autentikaciju transakcija male vrednosti. U tom slučaju postoje različiti pristupi: MasterCard uvek zahteva mPIN, dok Amex i Visa dozvoljavaju vršenje transakcija male vrednosti bez unosa mPIN-a. U zavisnosti od rizika i politike koja reguliše zloupotrebe, izdavalac kartice ili sam korisnik mogu dozvoliti izvršavanje transakcija male vrednosti bez unosa mPIN-a ili se može sprovesti upotreba mPIN-a u svim situacijama, bez obzira na iznos transakcije.

Važno je napomenuti da je mPIN postavljen za proces aktivacije i nije direktno povezan sa kredencijalima za plaćanje.

mPIN se nikada ne verifikuje od strane samog uređaja, ali uneta vrednost je kriptovana i proverava se online od strane ISP C sistema kao deo procesa autorizacije transakcije. U postupku autorizacije transakcije, transakcije izvršene virtuelnim platnim karticama se u back office sistemu obrađuju identično kao i sve druge kartičarske transakcije uz naznaku da se radi o beskontaktnim transakcijama.

Moguće je podesiti aplikaciju Digitalnog novčanika tako da je za svaki prijavljeni proizvod potrebno uneti različit mPIN, ali je preporuka procesora da se isti mPIN koristi za sve proizvode prijavljene za Wave2Pay uslugu. U isto vreme mPIN se može koristiti za pristup aplikaciji Digitalnog novčanika ili za aktivaciju/deaktivaciju nekih od opcija aplikacije. U tim situacijama zvaće se passcode, ali je vrednost ista.

3.4 *Kredencijali za plaćanje*

Kredencijali za plaćanje u aplikaciji Digitalnog novčanika sadrže PAN (Primary Account Number), opciono šifrovan mPIN (prema zahtevima platne šeme) i dodatne bezbednosne elemente.Kada se uređaj prinese POS terminalu, platnim kredencijalima se pridružuju podaci o trgovcu i iznos transakcije (slika 3). Takvi platni kredencijali su kompletni i šalju se sistemu za obradu kako bi se autorizovala tranakcija i verifikovao mPIN. U slučaju da je otisak prsta zamenio mPIN, sistem za autorizaciju vrši kontrolu samo ukoliko je otisak prsta ispravan.

Slika 3. *Platni kredencijali*

Platni kredencijali su u osnovi podeljeni na:

- Jednokratne i
- Kredencijale za višekratnu upotrebu.

Jednokratni kredencijali su dizajnirani samo za jednokratnu upotrebu, u smislu validnosti samo za jednu kartičarsku transakciju. Kao mera sigurnosti, važnost jednokratnih kredencijala je vremenski ograničena, što dovodi do toga da se kredencijali brišu nakon njihove eksploatacije za pojedinačnu kartičarsku transakciju ili nakon isteka vremena za korišćenje. Kada se iskoriste ili isteknu, kredencijali se brišu i ne mogu se ponovo koristiti.

Kredencijal za višekratnu upotrebu se može koristiti više puta u okviru unapred definisanog vremenskog okvira važnosti, što bi značilo da bi jedan kredencijal bio validan za više od jedne kartičarske transakcije tokom perioda važenja kredencijala. Nakon što istekne vreme važenja kredencijala, on je nevalidan i ne može se ponovo koristiti.

Deo platnog kredencijala koji se višestruko koristi je uvek onaj koji je kreiran od strane Digitalnog novčanika. U zavisnosti od podešavanja koja se odnose na rizik i zloupotrebe, šifrovana vrednost mPIN-a sa istim platnim kredencijalima koja se koristi za prvu transakciju može se koristiti i za druge transakcije. Alternativno, aplikacija Digitalnog novčanika bi mogla forsirati i unos mPIN-a sa istim platnim kredencijalima prilikom svake transakcije.

Svi prethodno navedeni kredencijali se dalje mogu podeliti na:

- Online i
- Offline.

Online platni kredencijali predstavljaju jednokratne platne kredencijale koji se mogu dobiti svaki put iz cloud-a kada korisnik inicira plaćanje. To bi značilo da bi mobilni uređaj trebalo da ima omogućen prenos podataka. Takvi kredencijali se ne čuvaju trajno na uređaju, već postoje na njemu ograničeni vremenski period i mogu se koristiti jednokratno ili višestruko kako je to ranije opisano.

Offline platni kredencijali se preuzimaju iz cloud-a i čuvaju na uređaju. Uređaj može čuvati nekoliko platnih kredencijala u svom repozitorijumu. Ovi kredencijali se čuvaju neaktivni i kada korisnik inicira plaćanje, kredencijali se uzimaju iz repozitorijuma i aktiviraju (aktiviranje kredencijala može biti jednokratno ili višekratno). Tokom iniciranja plaćanja, opcija za prenos podataka na uređaju nije neophodno da bude aktivna, ali jeste prilikom preuzimanja kredencijala.

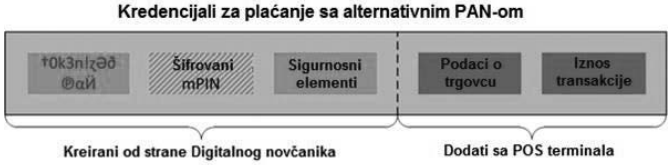
Svaki prijavljeni HCE proizvod u Wave2Pay servisu će imati sopstveni platni kredencijal koji će se menjati kada mu istakne period važenja ili kada se iskoriste raspoložive transakcije. Održavanjem platnih kredencijala upravlja aplikacija Digitalnog novčanika koja obaveštava korisnika o isticanju ili upotrebi platnih kredencijala za sve prijavljene proizvode.

Kompletno ISPC rešenje omogućava korišćenje višekratnih offline platnih kredencijala. Osim toga, takvi kredencijali će biti ograničeni njihovom važnošću i brojem odobrenih transakcija čije će trajanje takođe biti vremenski ograničeno.

Na primer, offline platni kredencijali važe 7 dana i za 20 transakcija, pri čemu je izvršenje svake pojedinačne transakcije ograničeno na 1 minut. Ukoliko korisnik ne iskoristi kredencijale za izvršenje transakcije u okviru vremenskog ograničenja (na primer 1 minut), platni kredencijali će biti i dalje validni, ali će se broj raspoloživih transakcija smanjiti za 1 (na 19).

ALTERNATIVNI PAN

Tokenizacija se često koristi za procesiranje kreditnih kartica. Tokenizacija bi se mogla opisati kao proces zamene broja platne kartice alternativnom vrednošću koja se zove token. Detokenizacija je obrnuti proces i predstavlja prebacivanje tokena u njegovu alternativnu PAN vrednost. Sigurnost svakog tokena pojedinačno se oslanja prvenstveno na nemogućnost određivanja originalnog PAN-a koji predstavlja surogat vrednost (Slika 4). Postupak tokenizacije se sprovodi u momentu prijavljivanja klijenta za korišćenje usluge, dok se detokenizacija tokena vrši u momentu plaćanja, prilikom autorizacije transakcije.



Slika 4. *Platni kredencijali sa alternativnim PAN-om*

U mnogim kriptografskim aplikacijama se koriste generatori (pseudo)slučajnih brojeva. Generator (pseudo)slučajnih brojeva je algoritam koji vraća binarni niz, u kome nije moguće predvideti vrednost svakog sledećeg izlaznog bita na osnovu prethodnih bitova. ANSI X9.17 je jedan od standarda po kome se upravlja kriptografskim ključevima u okviru finansijskih institucija. Njegovi protokoli se koriste unutar finansijskih ustanova, kao što su banke, prilikom generisanja, manipulacije i distribucije kriptografskim ključevima [30].

Alternativni PAN u značajnoj meri povećava bezbednost i smanjuje mogućnost zloupotrebe, posebno kod transakcija koje su licem u lice kao što su e-commerce i MO/TO transakcije. On dodatno omogućava razvoj različitih funkcionalnosti koji omogućavaju povećanje zadovoljstva klijenata uslugom Digitalnog novčanika. Alternativni PAN se može koristiti nezavisno od platnih kredencijala, a ukoliko se kombinuje sa platnim kredencijalima on dolazi naposletku. Osim toga, alternativni PAN može biti jednokratni ili višekratni, samo kao platni kredencijal, ali ne može biti podešen online ili offline.

Tok plaćanja je skoro identičan platnim kredencijalima koji ne uključuju alternativni PAN. Jedina razlika je u detokenizaciji alternativnog PAN-a (u originalnu vrednost), što predstavlja dodatni korak u procesu autorizacije transakcija i odgovor o PAN se tek potom šalje POS terminalu.

4 ANALIZA POSTIGNUTIH REZULTATA

Evaluacija poslovnog modela je izvršena u formi upitnika na manjem uzorku kako bi se ispitalo zadovoljstvo testnih korisnika. Uzorak je u početnoj fazi činilo 25 korisnika koji su u produkcionom okruženju na POS terminalima na kojima je bilo moguće vršiti NFC komunikaciju mogli da testiraju aplikaciju Digitalnog novčanika. Promenom verzija aplikacije i uvođenjem procesa tokenizacije uzorak je sveden na 3 korisnika koji su aktivno testirali aplikaciju u produkcionom okruženju. Proces testiranja u pilot produkciji se sprovodi od marta ove godine.

Cilj testiranja usluge Digitalnog novčanika je utvrđivanje zadovoljstva korisnika prilikom izvršavanja mobilnog plaćanja na POS terminalima korišćenjem HCE tehnologije. Kriterijumi evaluacije implementiranog rešenja se pre svega odnose na upotrebljivost, satisfakciju i jednostavnost u korišćenju aplikacije Digitalnog novčanika:

- Korisnost,
- Efikasnost
- Ušteda vremena,
- Fleksibilnost,
- Bez nedoslednosti,
- Jednostavan za upotrebu,
- Zadovoljstvo aplikacijom.

Korisnicima je putem elektronske pošte prosleđen upitnik sa pitanjima po prethodno definisanim kriterijumima i ocenama rangiranim od 1 do 7. Ocena 1 je značila potpuno nezadovoljan, dok je ocena 7 bila sasvim zadovoljan. Pitanja su se odnosila na korišćenje HCE usluge.

Pitanje	Prosečna ocena
Pomaže mi da budem efikasniji	6,67
Korisna je	6,67
Jednostavna za korišćenje	6,33
Zadovoljava sve moje potrebe	6,67
Mogu uspešno da je koristim u svako doba	5,33
Brzo sam naučio da je koristim	6,33
Zadovoljan sam uslugom	6,33
Preporučio bih je drugima	7,00

Tabela 2. *Deo rezultata anketiranih korisnika*

Rezultati ispitanog uzorka pokazuju da su svi korisnici zadovoljni efikasnošću i produktivnošću koju ostvaruju i da rešenje ispunjava sva njihova očekivanja. Što se tiče korišćenja aplikacije, sa najvećim ocenama su ocenjena lakoća u rukovanju, jednostavnost, minimalan uloženi trud prilikom korišćenja i prilagođenost korisnicima. Zanemarljivo nižu ocenu je dobila aplikacija po pitanju fleksibilnosti, jer su sva podešavanja unapred predefinisana bez mogućnosti da korisnik promeni neko od njih. Svi ispitani korisnici su se izjasnili najvišom ocenom po pitanju zadovoljstva prilikom korišćenja i preporučili bi je prijateljima.

Niska ocena je iskazana na pitanje da li se Wave2Pay aplikacija može uspešno koristiti u svako doba. Korisnici su ocenili nižim ocenama aplikaciju po ovom pitanju zbog nemogućnosti korišćenja aplikacije na svim POS terminalima. U prvoj fazi Virtuelna Banca Intesa AD Beograd platna kartica će moći da se koristi na 30% POS terminala u Srbiji, koji predstavljaju jednu od najvećih POS mreža u Srbiji. Plan je da se do jula 2017. godine čitava mreža POS terminala u vlasništvu Banca Intesa unapredi u smislu da će svi POS uređaji omogućavati bežične transakcije.

Pozitivni pokazatelji sprovedene evaluacije poslovnog modela su pre svega visoke ocene koje je aplikacija dobila na pitanja o efikasnosti, lakoće u rukovanju i korisnosti. Generalno mišljenje je da su korisnici u većini zadovoljni funkcionalnostima koje Digitalni novčanik ima.

5 ZAKLJUČAK

Uvođenje usluge Digitalnog novčanika ima za cilj kreiranje inovativnih poslovnih modela i servisa primenom savremenih informacionih tehnologija i bezbednosnih standarda. Neposredna primena novih tehnologija u bankarskom sektoru omogućila je razvoj novih bankarskih proizvoda i usluga čija primena će dovesti do strukturnih transformacija u kanalima distribucije, postizanje konkurentske prednosti, unapređenja tržišnog nastupa i asortimana bankarskih proizvoda.

Novi model poslovanja će uvesti novine u oblasti mobilnog bankarstva, a njegove osnovne prednosti su:

- Pogodan za brza bežična mobilna plaćanja,
- Lak i jednostavan za korišćenje,
- Kupovina korišćenjem virtuelne kartice,
- Uvid u stanje na klijentovom mobilnom telefonu,
- Mogućnost dodavanja dodatnih kartica u budućnosti,

- Isplata gotovine u budućnosti,
- Odobravanje e-commerce transakcija u drugoj fazi [31][32].

Primarni cilj implementacije projekta Digitalnog novčanika je da puštanjem u produkciju Wave2Pay usluge za vršenje beskontaktnih plaćanja korišćenjem mobilnih telefona izvrši akviziciju novih klijenata, kao i migraciju korisnika na digitalne kanale poslovanja. Servis će u narednim fazama obezbediti i dodatne funkcionalnosti kao što su mogućnost dodavanja drugih virtuelnih kartica u novčanik, podizanje gotovine, potvrda transakcija elektronske trgovine, itd.

Banca Intesa je pionir u razvoju digitalnog bankarstva na domaćem tržištu i uvođenje Wave2Pay usluge tokom 2016. godine je početak novog platnog metoda koji će uticati na povećanje nivoa digitalizacije bankarskog sistema u Srbiji.

REFERENCE

[1] Republički zavod za statistiku, „Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2015.", 2015.
[2] The Statistics Portal Statista, Research: Number of NFC-enabled mobile devices worldwide from 2012 to 2018 (in million units), 2016.
[3] Visa Europe, Report: Smart devices on track to replace cash and cards, 2015.
[4] D. A. A. Ali, Journal of Library and Information Sciences, Near-Field Communication Technology and Its Impact in Smart University and Digital Library: Comprehensive Study, 3(2), pp: 2-13, ISSN 2374-2372, 2015.
[5] B. Radenković, M.Despotović-Zrakić, Z.Bogdanović, D.Barać, A.Labus, Elektronsko poslovanje, Faculty of organizational sciences, pp 266-271, ISBN:978-86-7680-304-0, 2015.
[6] J. Vasković, InfoM, NFC tehnologija i mogućnosti njene praktične primene, ISSN 1451-4397, 2012.
[7] Gemalto, http://www.gemalto.com/mobile/mcommerce/nfc, 7 myths about mobile NFC
[8] G. Arcese, G. CAmpagna, S. Flammini, O. Martucci, Near Field Communication: Technology and Market Trends, pp 143-163, ISSN 2227-7080, 2014.
[9] Oracle Corporation, http://www.oracle.com/technetwork/articles/javame/nfc-140183.html, An Introduction to Near-Field Communication and the Contactless Communication API, 2008.
[10] K. Curran, A. Millar, C. M. Garvey, International Journal of Electrical and Computer Engineering (IJECE), Near Field Communication, 2(3), ISSN: 2088-8708, 2012.
[11] S. H. Wu, C. Yang, A Study on Designing the New Near Field Communication Technology-NFC-micro SD Technology, Information Technology Journal, 13(7), ISSN 1812-5638, 2013.
[12] NFC Forum, Essentials for Successful NFC Mobile Ecosystems, 2008.
[13] Vibhor Sharma, Preeti Gusain, Prashant Kumar, Near Field Communication in Conference on Advances in Communication and Control Systems (CAC2S 2013), pp. 342-345, 2013..
[14] NFC World +, http://www.nfcworld.com/technology/mobile-banking/, Visa Europe adds support for cloud-based credentials to tokenization service, 2016.
[15] Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure, Smart Card Alliance Contactless Payments Council, CPC, 2007.
[16] N. Prakash, Host Card Emulation, International Journal of Scientific and Research Publications, 5(8), ISSN 2250-3153, 2015
[17] Association Francaise du Sans Contact Mobile, Introduction to afscm mobile NFC service specifications, AFSCM, 2009.
[18] J. Vasković, Magazin: Bankarstvo, izdanje 4, Primena NFC tehnologije u sistemima plaćanja, 2012.
[19] G. Arcese, G. CAmpagna, S. Flammini, O. Martucci, Near Field Communication: Technology and Market Trends, pp 143-163, ISSN 2227-7080, 2014.
[20] Smart Card Alliance, Host Card Emulation (HCE) 101, A Smart Card Alliance Mobile & NFC Council white paper, MNF-CC-14002, 2014.
[21] A. Ahmad, R. Iqbal, D. Saeed, International Journal of Computer Science and Artificial Intelligence, Emulation of Multi-application Contactless Smartcard in Near Field Communication Enabled Smart Phones, 5(1), DOI: 10.5963/IJCSAI0501002, 2015.
[22] S.Pannifer, D. Clark, D. Birch, HCE and SIM Secure Element: It's not black and white, A Discussion Paper from Consult Hyperion, http://www.chyp.com/wp-content/uploads/2015/01/HCE-and-SIM-Secure-Element.pdf ,2014.
[23] P. Pourghomi, P. E. Abi-Char, G. Ghinea, International Journal of Computer Science and Information Security (IJCSIS), Towards a mobile payment market: A Comparative Analysis of Host Card Emulation and Secure Element, 13(2), ISSN 1947-5500, 2015.
[24] Banca Intesa AD, Functional Specification for Wave2Pay service, 2015.
[25] SANS Institute InfoSec Reading Room, Security of Mobile Banking and Payments, dostupno na https://www.sans.org/mwg-internal/de5fs23hu73ds/progress?id=_QoGKcPyYK6fEi5IUeaMHmo-8iDlOZ2P_M2WnNU3H88M,&dl, 2012.
[26] Intesa Sanpaolo Card, Cloud Tokenization, 2016.
[27] Intesa Sanpaolo Card, Product Definition – BIB NFC HCE Visa Inspire, 2014.
[28] Intesa Sanpaolo Card, Process Overview – BIB Mobile Wallet, 2014.
[29] Privredna Banka Zagreb Wave2Pay, http://wave2pay.pbz.hr/
[30] M. Štampar, Diplomsi rad: Ocjena kvalitete algoritama za šifriranje statističkim testiranjem generatora pseudo-slučajnih brojeva, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, 2005.
[31] M. Anshari, Y. Alas, The Journal of High Technology Management Research: Smartphones habits, necessities, and big data challenges, 26(2), pp 177-185, 2015.
[32] G. Jain, S. Dahiya, NFC: advantages, limits and future scope, International Journal on Cybernetics & Informatics (IJCI), 4(4), 2015.

Dragana Vasiljević, Banca Intesa ad Beograd
Kontakt: dragana.vasiljevic@bancaintesa.rs
Oblasti interesovanja: elektronsko bankarstvo, mobilno bankarstvo, e-commerce

Prof. dr Zorica Bogdanović, Fakultet organizacionih nauka, Beograd
Kontakt: zorica@elab.rs
Oblasti interesovanja: elektronsko poslovanje, mobilno poslovanje, Internet tehnologije

Aleksandra Vukmirović, Fakultet organizacionih nauka, Beograd
Kontakt: aleksandra.vukmirovic@stata.rs
Oblasti interesovanja: elektronsko poslovanje, internet marketing