Uporaba brezkontaktnih kartic za namene brezgotovinskega plačevanja na prireditvah

Matjaž Fras[1], Peter Šamperl[1], Amor Chowdhury[1,2]

[1]*Margento R&D, Gosposvetska cesta 84, 2000 Maribor*
[2]*Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija*
E-pošta: matjaz.fras@margento.com

Using contactless cards for cashless payments for events

This article describes Margento cashless payment system for concerts or other closed social events. The main benefit of developed system is using the contactless smart cards based on NFC tehnology instead of cash or even coupons at concert or other social events. The system allows create event contactless cards, charging the credit at virtual accounts at contactless cards and then buying goods and services at different spots of event from the virtual account. System contains three main parts. The first is a contactless smart card (MIFARE Classic or MIFARE DESFire). The second part of the systems presents Margento, which are used for contactless card communication and receipt printing. Last part of the system is a processing platform, which is used for storing transaction data, terminal management, card management and report generation. Every action on card is automatically logged and sent to Margento processing platform for further analysis or report generation.

1 Uvod

Brezkontaktne kartice postajajo naš vsakdanj, saj se le te vsakodnevno uporabljajo na najrazličnejše načine kot je npr. identifikacija ali plačevanje najrazličnejših storitev in dobrin. V zadnjih letih so se brezkotnaktne kartice pojavile tudi na različnih družabnih dogodkih in glasbenih festivalih, kjer se je uvedel tako imenovan sistem brezkontaktnega poslovanja za obiskovalce prireditve. Takšen sistem je zaradi svojih prednosti (hitrejše nakupovanje, večja preglednost denarnega toka,...) nadomestil zamudno in nepregledno poslovanje z gotovino na prodajnih mestih družabnega dogodka ali pa sistem z nakupom in koriščenjem kuponov, ki jih je bilo mogoče kupiti ter nato koristiti. Koncept uporabe brezkotnaktnih kartic na glasbenih festivalih ali drugih družabnih prireditvah in dogodkih temelji na zaprtem elektronskem sistemu plačevanja storitev, ki temelji na tehnologiji NFC (Near field communication). V takšnem sistemu se kot plačilni medij uporablja brezkotnaktna kartica, ki jo uporabljajo obiskovalci kot plačilno sredstvo. Poleg plačilne kartice se v sistemu uporabljajo tudi različni čitalci (terminali, tablice) s podprto tehnologijo NFC, ki omogočajo komunikacijo s brezkotnaktnimi karticami.

V našem podjetju smo razvili zaprti elektronski sistem plačevanja storitev za festivale ali družabne dogodke na osnovi NFC tehnologije. V plačilnem sistemu smo uporabili kot:

- Medij – brezkontaktna pametna kartica tipa Mifare Classic ali Mifare Desfire
- Plačilni Terminal – Margento terminal, ki lahko služi kot samostojna blagajna, ki natisne račun, prav tako pa je lahko integrirana z že obstoječo blagajno in predstavlja čitalec brezkontaktnih kartic.
- Procesni center – shranjevanje vseh transakcij ter generiranje najrazličnejših poročil (transakcije, izdaja kartic,...), vodenje črne liste brezkotnaktnih kartic, posobitve programske opreme terminala.

V nadaljevanju članka bomo opisali posamezne segmente razvitega zaprtega elektronskega sistema plačevanja storitev za družabne dogodke na osnovi NFC tehnologije.

2 Tehnični opis sistema

Razvit zaprt elektronski sistem plačevanja storitev za družabne dogodke na osnovi NFC tehnologije omogoča nalaganje denarja na brezkontaktno pametno kartico na osnovi RFID tehnologije [1] kot dobroimetje ter koriščenje dobroimetja za nakup določenih storitev in dobrin na posebnih mestih koriščenja. Brezkotnaktno kartico je mogoče pridobiti na glavni blagajni oz. info točkah, na katerih si je mogoče naložiti dobroimetje. Znesek, ki je na kartico naložen se lahko porabi le za nakup znotraj območja festivala na prodajnih mestih. Zaprti elektronski sistem za elektronsko plačevanje deluje vedno v »offline« načinu, kjer si bodo terminali pridobili le posodobitve in črne liste kartic. Tako blagajne, info točke in prodajna mesta so opremljena z Margento terminali [2], ki podpirajo NFC tehnologijo [3], kar pomeni, da je z njimi mogoče branje podatkov in pisanje podatkov na brazkotnaktno kartico. Prav tako

terminali podpirajo GPRS povezavo s procesnim centrom, na katerega pošiljajo informacije o transakcijah (nova kartica, nalaganje dobroimetja, plačilo,...) [4].

2.1 NFC tehnologija

NFC ali Near Field Communication [3, 4] predstavlja visokofrekvenčno komunikacijsko tehnologijo kratkega dosega, ki se je v zadnjih letih pojavila na mobilnih telefonih in brezkotnaktnih karticah za uporabo na različnih področjih, kot to kontrola dostopa, identifikacijo, plačevanje ter različnih bonusnih programih. NFC tehnologija je skupek standardov, ki omogočajo komunikacijo in izmenjavo podatkov med dvama napravama na krajših razdaljah (nekaj centimetrov) preko radijskih valov. NFC standard pokriva komunikacijske protokole in formate izmenjave podatkov na osnovi obstoječih RFID (Radio-Frequency IDentification) [3] standardov vključno s ISO/IEC 14443[5] in FeliCa[6]. Standardi vključujejo ISO/IEC 18092 in standardne definirane s strani NFC Foruma, ki je nastal leta 2004 strani Nokia-je, Philips Semiconductors (od 2006 NXP Semiconductors. NFC komunicira prek magnetnega polja, kjer se anteni nahajata znotraj medsebojnega bližnjega polja in tako predstavljata transformator z zračnim jedrom. Deluje znotraj ISM-radiofrekvenčnega pasu 13,56 MHz s pasovno širino 2 MHz. Podprte hitrosti prenosa podatkov: 106, 212, 424 in 848 kbit/s.

NFC tehnologija podpira dva načina delovanja in sicer pasivni in aktivni [3]. Pasivni način: inicialna naprava omogoča nosilno polje, ciljna naprava odgovori z modulacijo obstoječega polja, pri čemer jo to polje tudi napaja. Aktivni način: inicialna in ciljna naprava komunicirata z izmenjujočim generiranjem lastnega polja. Naprava izključi lastno RF-polje, medtem ko čaka na podatke. V tem načinu potrebujeta obe napravi izvor napajanja.

Področja uporaba NFC tehnologije:

- Identifikacija,
- Kontrola dostopa,
- Prisotnost na delu,
- Logiranje,
- Transport
- Brezgotovinsko plačevanje,
- Vstopnice,
- Bonusni programi, članstvo.

2.2 Terminal Margento

V razvitem zaprtem elektronskiem sistemu plačevanja storitev za družabne dogodke,Margento terminal [2] predstavlja napravo, ki podpira NFC tehnologija [3] in omogoča branje (npr. dobroimetje) ter pisanje podatkov na brezkotnakne kartice (npr. novo stanje dobroimetja po plačilu). Terminal omogoča najrazličnejše storitve, kot so plačevanje ter identifikacijo s pomočjo mobilnega telefona DOV (Data Over Voice) ali brezkontaktne kartice na osnovi NFC. Terminal omogoča prenos ustreznih tipov transakcij glede na opravljene storitve z različnimi komunikacijskimi tehnologijami, kot je GPRS (General Packet Radio Service), Ethernet, govorni kanal mobilnega omrežja, itd. Terminal je zasnovan na sistemu mobilnih transakcij, kjer se prenos podatkov izvede preko govornega kanala različnih mobilnih komunikacijskih sistemov kot so GSM, CDMA in UMTS, kar predstavlja izvirno rešitev [8].

Slika 3 prijazuje Margento terminal mPOS T4500 s podprto tehnologijo NFC za branje brezkontaktnih kartic.

Slika 2. Margento terminal mPOS 4500 s podprto NFC tehnologijo za branje brezkontaktnih kartic.

2.3 Aplikacija na Margento terminalu:

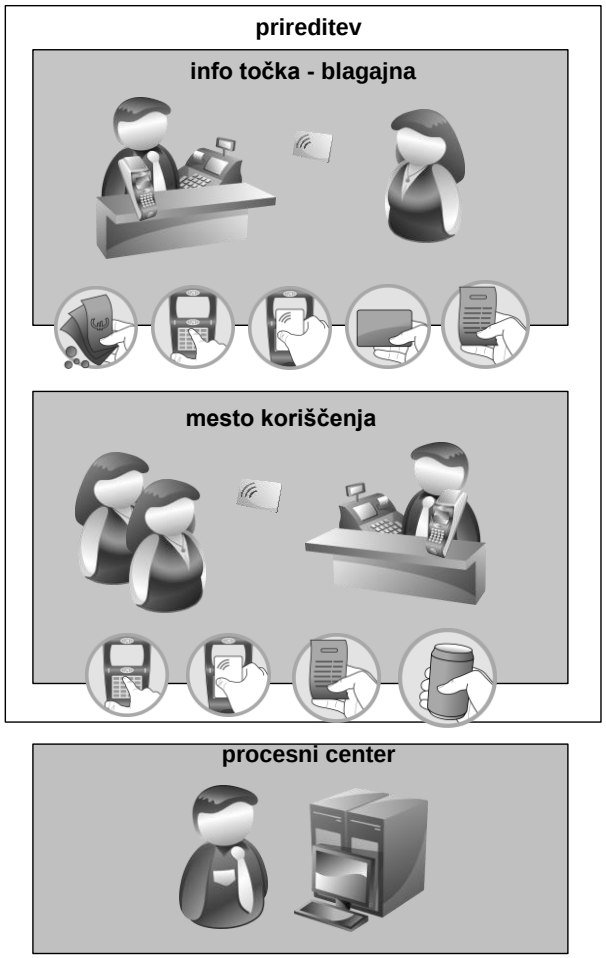
Na terminalu T4500 je bila za namene elektronskega sistema plačevanja storitev za festivale ali družabne dogodke razvita aplikacija, ki omogoča:

- Izdelava kartice za določen festival ali dogodek (npr. čas veljave,...).
- Nalaganje dobroimetja na kartico.
- Plačilo soritve iz dobroimetja na kartici.
- Stornacija zadnje transakcije.
- Preverjanje stanja dobroimetja na brezkontaktni kartici.
- Pošiljanje podatkov o transakcijah na procesni center.
- Generiranje poročil.

Aplikacija je zasnovana tako, da omogoča blagajniku na info točki-blagajni izdajo brezkotnaktne kartice uporabniku. Pri tem se na kartico s pomočjo terminala Margento T4500 zapišejo vsi potrebni podatki o dogodku, o času veljav, ... Prav tako lahko uporabnik napolni dobroimetje na kartici, ki ga lahko nato koristi na mestih koriščenja. Mesta koriščenja so prav tako kot

info točke opremljenje z Margento terminali, ki omogočajo plačilo storitev in dobrin (hrana, pjača) iz dobroimetja na kartici. Pred samim nakupom blagajnik vnese znesek nakupa, nato pa uporabnik (kupec) prisloni kartico k terminalu. Po uspešni transakciji, se na kartici odšteje znesek nakupa od dobroimetja, na terminalu pa se natisne račun nakupa. Prav tako je na terminalu možno izvesti stornacijo zadnje transakcije.

Slika 3 prikazuje uporabo brezkontaktnih kartic za namen polnjenja in koriščenja dobroimetja na prireditvah, kjer so info točke - glavna blagajna in mesta koriščenja opremnljena z Margento terminalom.



Slika 3. Celoten sistem za uporaba brezkontaktnih kartic za namen polnjenja in koriščenja dobroimetja na prireditvah

2.4 Procesni center

Razvit sistem deluje v »offline« načinu, kar pomeni, da se transakcije (plačilo, polnitev) ne pošiljajo v realnem času na procesni center, ampak se to izvede po določenem času. Podatki na procesnem centru nam služijo za generiranje najrazličnejših tipov poročil in sicer po meri naročnika.

Tipi podprtih poročil:

- Poročila o vseh transakcijah: polnitve/izdaja kartic/poraba/info
- Finančna poročila: polnitve/izdaja kartic/poraba
- Število polnitev in porabe po posameznem prodajnem mestu prodaje/terminalu

Prav tako nam zbrani podatki o transakcijah, koristijo za generiranje tako imenovane črne liste kartic, ki se prenaša na terminale in omogoča izločitev (blokiranje) kartic v primerih zlorabe.

3 Brezkontaktne kartice

Brezkontaktne pametne kartice[9] so velikosti običajnih kreditnih kartic z vgrajenim integriranim tiskanim vezjem, ki omogočajo predvsem varno shranjevanje in hitro izmenjavo podatkov na osnovi radijskih valov z zelo dolgo življensko dobo. Brezkontakne kartice so postale naš vsakdanj, saj se uporabljajo za osebno identifikacijo (kontrola dostopa), plačevanje storitev znotraj zaprtih plačilnih shem (transport) ter tudi v obliki brezkontaktnih kreditnih in debit kartic (PayPass-MasterCard, payWay- Visa).

Kartice lahko ločimo v dve skupini in sicer na aktivne in pasivne. Na aktivne kartice na katere je mogoče zapisovati podatke, ter podatke tudi spreminjati ali pa brisati. Na pasivne kartice ni mogoče zapisovati podatkov ampak jih je možno samo brati. Osnovna sestavina brezkotnakne kartice je brezkontaktni mikročip in antena, ki zagotavlja električni tok za napajanje. Osnovno zgradbo brezkontakne kartice prikazuje naslednja slika 4.

Slika 4. Zasnova brezkontaktne kartice (antena in mikročip)

Poznamo več različnih brezkontaktnih mikročipov, ki delujejo na različnih frekvencah (13.56MHz, 125kHz, 127kHz,...). Med najbolj pogosto uporabljenimi so Mifare(13.56MHz), HID(13.56MHz ali 125kHz), FeliCa(13.56MHz)in EM(125kHz).

Komunikacija za brezkontaktne pametne kartice je predpisano s standardom ISO/IEC 14443, ki definira dva tipa brezkontaktnih kartic in sicer Tip A in Tip B [3], ki omogoča komunikacijo na razdalji do 10cm.

Brezkotnaktne kartice so se zažele uporabljati kot elektronske kartice leta 1995 v Seoulu. Primeri široke

uporabe brezkontaknih kartic so še Taiwan's EasyCard, Hong Kong's Octopus card, Shanghai's Public Transportation Card, South Korea's T-money , London's Oyster card, Beijing's Municipal Administration and Communications Card...

3.1 Brezkontaktne kartice MIFARE

Na tržišče je danes veliko brezkontaknih pametnih kartic z različnimi karakteristikami različnih proizvajalcev. V našem podjetju največ uporabljamo pametne kartice Mifare[11, 12]. Brezkontakne pametne kartice MIFARE predstavljo blagovno znamko brezkontaktnih plačilnih kartic NXP podjetja. NXP podjetje (spin off podjetje nizozemske corporacije Phillips) predstavlja eno od vodilnih proizvajalcev brezkontalnih kartic v svetu. Mifare pokriva več različnih tehnologij brezkontakntih kartic na osnovi standarda ISO/IEC 14443 in sicer za Tip A kartice za frekvenco 13.56 MHz. Tako je na voljo več različnih brezkontaktnih kartic MIFARE in sicer:

- MIFARE Classic
  skladen s deli standarda (ne vsi deli) ISO/IEC 14443-3 za A tip kartice, z NXP varnostnimi protokoli za avtentifikacijo in šifriranje.
- MIFARE Ultralight
  nizkocenovna in skladna s protokolom .ISO/IEC 14443-3 za A tip kartice.
- MIFARE Ultralight C
  nizkocenovna in primerna za aplikacije omejene rabe, ki ponujajo Triple Des kriptografijo.
- MIFARE DESFire
  pametna kartica skledna s standardom ISO/IEC 14443-4 za tip A kartico z NXP operacisjkim sistemom.
- MIFARE DESFire EV1
  enako kot predhodna kartica vendar še vsebuje AES enkripcijo.
- MIFARE DESFire EV2
  enako kot predhodna kartica ampak še podpira MIsmartApp, Transaction MAC, Unlimited Applications.
- MIFARE Plus
  nadomestilo za kartice MIFARE Classic z določenimi izbolšavami glede varnosti (AES 128)
- MIFARE SAM AV2
  omogoča varno hranjenje kriptografskih ključev in kriptografskih funkcij

V našem primeru smo za predstavljeno aplikacijo uporabe brezkontaktnih kartic za namen polnjenja in koriščenja dobroimetja na prireditvah uporabili MIFARE Classic brezkontaktne kartice, ki predstavljajo najcenejšo varianto MIFARE brezkontaktnih kartic. Vendar se pa moramo ob tem zavedati tudi njehovo pomankljivost v varnosti [7, 13], katere so bile pokazane v različnih primerih. Zaradi teh slabosti in opravljenih testih se v našem primeru poslužujemo MIFARE DESFire EV1 brezkotnaktnih kartic, ki predstavljajo veliko bolj varno rešitev ampak tudi dražjo.

4 Sklep

Razvit sistem se je tekom različnih družabnih dogodkov pokazal veliko prednosti v primerjavi z zamudnim gotovinskim poslovanjem ali pa s sistemom nakupa in unovčevanja kuponov. Prednosti takšnega sistema so predvsem s stališča hitrejšega nakupa ter tudi s transparentnostjo denarnega toka. V nadaljevanju projekta je cilj podpora uporabe NFC telefona kot nadomestilo za brezkontakno pametno kartico. To pomeni da si na NFC naložimo virtualno karto družabnega dogodka ter nato nalaganje dobroimetja, ki ga lahko nato obiskovalec uporablja znotraj dogodka na mestih koriščenja. Prav tako bi na telefonu lahko razvili aplikacijo kjer lahko uporabnik spremlja svoje dobroimetje na virtualni kartici ter pridobi dodatne koristne informacije o sami prireditvi.

Literatura

[1] J. Kroflič, A. Chowdhury, B. Kotnik in R. Svečko, RFID tehnologija na podrocju pametnih kartic, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[2] M. Kseneman, F. Horvat in A. Chowdhury, Modularna zasnova programske opreme plačilnega terminala – mPOS T4500, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[3] NFC wikipedia: http://en.wikipedia.org/wiki/Near_field_communication

[4] Andrej Medved, Amor Chowdhury, Stanko Golicnik, Preizkušanje GPRS modemov ter razvoj mPOS tiskanine za vec GPRS modemov, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[5] Standard ISO/IEC_14443: http://en.wikipedia.org/wiki/ISO/IEC_14443

[6] FeliCa: http://en.wikipedia.org/wiki/FeliCa

[7] https://www.schneier.com/blog/archives/2008/08/hacking_mifare.html

[8] Ultra M-Pay patent 1 in 2, WO 02/33669, WO 03/088165, 2002

[9] A. Jurišić in A. Trojar, Pametna kartica (Smard card), Certicom Corp, Juanuar, 1997. http://lkrv.fri.uni-lj.si/popularizacija/pametne_kartice97.pdf

[10] http://www.cardusa.com/products/contactless-cards/

[11] http://www.mifare.net/en/home/

[12] http://en.wikipedia.org/wiki/MIFARE

[13] http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf