

UDK: 004.738.5:339

Stručni rad

INTERFEJS APLIKACIJA ZA PRAĆENJE TRANSAKCIJA KOD ELEKTRONSKOG PLAĆANJA

INTERFACE APPLICATION FOR THE MONITORING OF ELECTRONIC PAYMENT TRANSACTIONS

Nataša Gojgić¹, Marija Nikolić¹, Miodrag Stanišić¹¹Visoka škola tehničkih strukovnih studija Čačak

natasa.gojgic@vstss.com, marija.nikolic@vstss.com, miodrag.stanistic@vstss.com

Apstrakt: U poslovanju savremenih maloprodajnih objekata javlja se potreba za lakšim i sigurnijim korišćenjem PoS terminala koji služe za bezgotovinsko elektronsko plaćanje karticama. Pre svega potrebno je rad PoS terminala što više integrisati u postojeći informacioni sistem da bi se ubrzao rad i smanjio broj grešaka. Za ostvarivanje ovog cilja potrebna je fizička konekcija između PoS terminala i elektronske kase i odgovarajući softverski interfejs.

U radu je prikazano povezivanje PoS terminala i softvera za elektronsku kasu ECR.

Ključne reči: transakcije elektronskog plaćana, Pos terminal, ECR interfejs aplikacija

Abstract: In business activities of the retail objects there is a need for easier and safer usage of Pos- terminals which are used for cashless electronic payment by cards. First of all, it is necessary to integrate the Pos working processes as much as possible into the existing information system in order to speed up working process and decrease the number of errors. For fulfilling this goal, physical connection between the Pos terminal and electronic cash registers and the corresponding software interface are necessary. This paper presents connecting of the Pos terminal and the software for the electronic cash registers ECR.

Key words: electronic payments transactions, Pos terminal, ECR interface application

1. UVOD

Informacione tehnologije značajno unapređuju obavljanje finansijskih transakcija koje se sada mogu obavljati mnogo brže, tačnije, pouzdanije i udobnije nego ranije. U savremenim uslovima tradicionalni način plaćanja sve više gubi na značaju, a prednost se daje elektronskom načinu plaćanja.

2. INFRASTRUKTURA ZA ELEKTRONSKO PLAĆANJE

EFT / PoS je skraćeno od *Electronic Funds Transfer / Point of Sale*, što možemo prevesti kao elektronski transfer sredstava / mesto prodaje i predstavlja sistem bezgotovinskog plaćanja u kom su elektronske kase-terminali direktno povezani sa poslovnim bankama.

Fiskalna kasa je uređaj na kojem su podaci o ostvarenom prometu i softver posebno zaštićeni od izmena i brisanja. Unos podataka obavlja se ili kucanjem šifre proizvoda putem tastature, ili pomoću čitača bar-koda. Kasa mora da ima i displej koji omogućava kupcu da prati šta se kuca.

2.1. NAČINI ZA FIZIČKU KONEKCIJU

Fizička konekcija se može realizovati preko:

- USB-a,
- RS-232,
- Ethernet-a,
- Wi-Fi-a,
- GPRS-a.

USB - PoS terminali se mogu povezati sa elektronskom kasom preko USB konekcije. Na ovaj način povezani terminali uspostavljaju virtualnu serijsku vezu ili PPP/TCP/IP preko virtualne serijske veze.

RS-232 (serial) - PoS terminali se mogu povezati sa elektronskom kasom preko RS-232 konekcije, ali tada PoS terminal mora imati posebnu TCP/IP konekciju, izuzetno PPP/TCP/IP veza se može ostvariti putem serijske konekcije.

Ethernet - PoS terminali se mogu povezati na LAN preko Ethernet-a. PoS terminali onda komuniciraju sa elektronskom kasom preko TCP/IP protokola putem lokalne mreže.

Wi-Fi - neki PoS terminali opremljeni su Wi-Fi konekcijom koja može zameniti Ethernet konekciju.

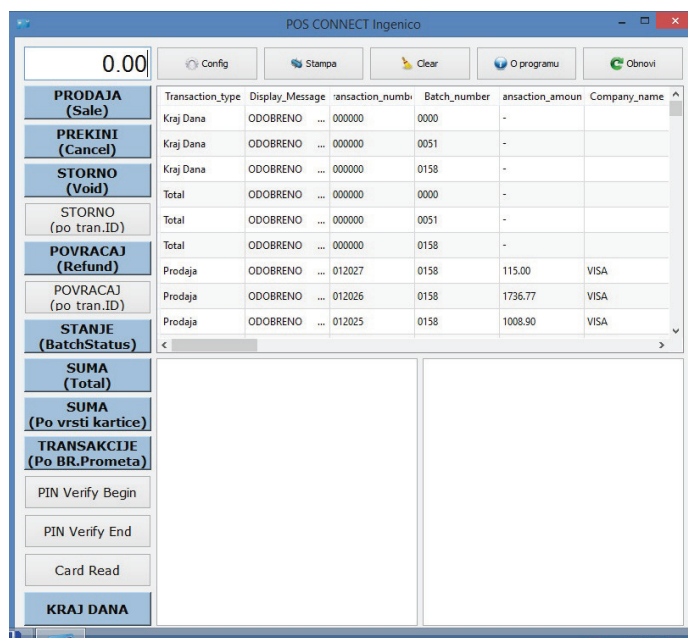
GPRS - PoS terminali ne koriste GPRS konekciju za komunikaciju sa elektronskom kasom, ali se njihova internet konekcija može koristiti za elektronsku kasu ukoliko ne postoji internet pristup.

2.2. INTERFEJS APLIKACIJA

Sve fiskalne kase, moraju imati terminal za daljinsko očitavanje dnevnih izveštaja, takozvani GPRS terminal (General Packet Radio Service). Kasa se može povezati i na običan računar, ali se mora koristiti sertifikovan softver.

Fiskalna kasa obavezno ima programsku, operativnu i fiskalnu memoriju. Programska memorija ima softver, koji je zaštićen od izmena ili brisanja, a koji koristi standardne

funkcije za evidentiranje prometa dobara i usluga, upravljanje radom štampača, ekrana i upisom podataka u fiskalnu memoriju. Operativna memorija sadrži bazu podataka o dobrima i uslugama i evidentiranim podacima o pojedinačnom prometu dobara i usluga. Softverski interfejs je aplikacija koja obavlja komunikaciju između PoS terminala i softvera na elektronskoj kasi, ECR (electronic cash register) interfejs aplikacija (slika 1).



Slika1: ECR interfejs aplikacija

3. POSTUPAK TRANSAKCIJE

Zakonom o fiskalnim kasama propisano je da je lice koje je upisano u odgovarajući registar za promet dobara na malo, odnosno za pružanje usluga fizičkim licima, dužno da vrši evidentiranje svakog pojedinačno ostvarenog prometa preko fiskalne kase.

Preko terminala daje se elektronski nalog računarskom centru banke da izvrši transfer novca sa računa kupca na račun prodavnice kada i počine postupak transakcije.

3.1. NAČINI KOMUNIKACIJE

Ovaj sistem omogućava direktan prenos sredstava sa računa kupca na račun prodavca. EFT / PoS terminali omogućavaju da se podaci sa kartice provere za manje od 15 sekundi u okviru mreže koja povezuje trgovce širom sveta sa centrom za obradu platnih kartica i emitentom kartice.

PoS terminali podržavaju tri načina komunikacije zavisno od fizičke konekcije:

- **Ethernet mode** - ovo je najjednostavniji i najfleksibilniji način povezivanja PoS terminala, koristi se kada PoS terminal ima fizičku ili wireless LAN

konekciju. IP adresa PoS terminala treba da bude konfigurisana u skladu sa zahtevima mreže. Uglavnom PoS terminali koriste port 5188.

- **PPP mode** - na ovaj način PPP konekcija se uspostavlja između PoS terminala i elektronske kase, a fizički preko USB-a ili serijske konekcije. PoS terminal će dalje koristiti TCP/IP vezu kao kod Ethernet veze.
- **Serial mode** - serijska komunikacija se koristi radi kompatibilnosti sa elektronskim kasama koje imaju samo mogućnost serijske komunikacije. U ovom slučaju PoS terminal mora imati zasebnu internet konekciju za host. Paketi u serijskoj komunikaciji su izolovani radi veće pouzdanosti.

3.2. FORMAT PAKETA I PORUKA

Svaki paket ima četiri dela početak (STX), deo sa podacima (message blok), oznaku za kraj paketa (ETX) i kontrolni karakter (LRC - Logitudinal redundancy check) koji se računa po standardu ISO1155 (tabela 1).

Tabela 1. Četiri dela paketa

STX	MESSAGE BLOK	ETX	LRC
1	Variable, 256 maksimum	1	1

Karakter koji se koriste u komunikaciji dati su tabeli 2.

Tabela 2. Specijalni karakteri u komunikaciji

Karakter	Hex vrednost	Značenje
STX	02	Početak teksta
ETX	03	Kraj teksta
EOT	04	Kraj prenosa
ACK	06	Pozitivan odgovor
NAK	15	Negativan odgovor

Postoje dve vrste formata poruka poruke u komunikaciji između elektronske kase i PoS terminala. Poruke koje se šalje elektronska kasa ka PoS terminalu su u formatu:

<STX><STX><Message DATA><ETX><LRC>.

Poruke od PoS terminala ka elektronskoj kasi su u formatu:

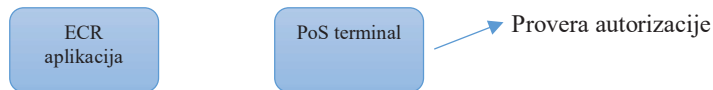
<STX><Message DATA><ETX><LRC>.

3.3 PREGLED TRANSAKCIJE

Potrošač koristi kreditnu ili debitnu karticu i preko terminala dolazi u on-line vezu sa kompjuterom banke koja je karticu izdala. Preko terminala daje se elektronski nalog računarskom centru banke da izvrši transfer novca sa računa kupca na račun prodavnice. U zavisnosti od vrste kartice, zahteva se i unos PIN-a od strane kupca, korisnika kartice.

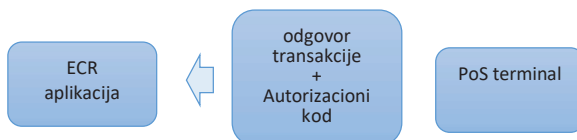
Kada se u eksternoj aplikaciji kreira zahtev za transakcijom prema PoS terminalu, PoS terminal porvrđuje zahtev pre započinjanja transakcije. PoS terminal analizira sadržaj zahteva unos nedostajućih podataka (npr. broj kartice) i pokreće proces autorizacije (npr. zahtev za PIN kodom).

Zatim se odvija proces provere autorizacije na odgovarajućem hostu koji vrši transaction management za detektovani tip kartice (slika 2).



Slika 2. Provera autorizacije

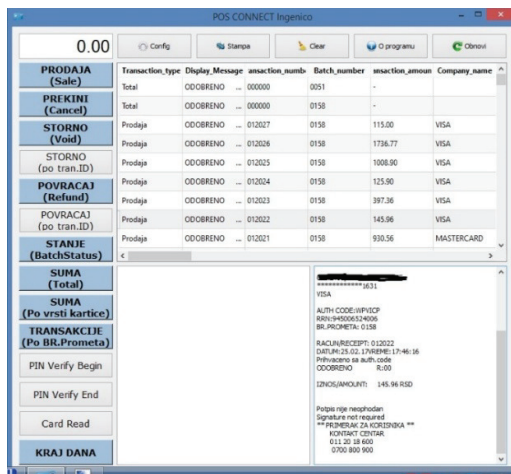
Nakon toga PoS terminal šalje opis transakcije nazad prema aplikaciji koji sadrži autorizacioni kod ili poruku o odbijanju transakcije (slika 3).



Slika 3. Rezultat transakcije

Na osnovu povratne informacije štampa se račun i to po pravilu u duplikatu, s tim što jedan primerak ostaje pružaocu usluge, odnosno prodavcu robe, dok se drugi daje kupcu uz fiskalni račun.

Pregled transakcija u interfejs aplikaciji dat je na slici 4.



Slika 4. Pregled transakcija u interfejs aplikaciji

Sva komunikacija se odvija u ASCII formatu i poruke su podeljene u više koraka čije su vrednosti i značenja dati u tabeli 3.

Tabela 3. Koraci pri komunikaciji

Vrednost	Značenje
00	Zahtev za transakcijom
10	Odgovor PoS terminala na zahtev (posle dobijenog 00 zahteva)
20	Hold (čekanje dok PoS terminal izvršava autorizaciju ili štamap slip)
22	Error (greška)

4. SIGURNOST PoS TERMINALA

Kada analiziramo sigurnost PoS (Point of Sale) aplikacija moramo uzeti u obzir korišćenje magnetnih traga i kartica koje sadrže podatke koji su izuzetno značajni, kako za korisnika tako i za instituciju koja ih koristi.

Kad god postoji potreba za zaštitom podataka, koriste se kriptografska rešenja. Izvorno razvijena u vojne svrhe, danas se koriste za zaštitu svih vrsta podataka. Korišćenje sigurnosnih protokala nije dovoljno samo po sebi, oni moraju biti tačno primenjeni i prilagođeni hardware-u i software-u.

Kao što se i predpostavlja, kriptografija je suštinska komponenta PoS terminala, kao i kod svih metoda elektronskog plaćanja koje se danas koriste. Dodatno, osnova poverljivosti i integriteta podataka leži u autentifikaciji (proveri identiteta) i neosporivosti, odnosno transakcija se ne može izvršiti bez znanja korisnika.

U elektronskom plaćanju najšire gledano postoje tri grupe kriptografskih algoritama koji se koriste u velikom broju rešenja samih PoS uređaja. Svaka grupa ima svoje prednosti i mane. Razlike se najviše ogledaju u potrošnji energije, brzini i lakoći primene u različitim delovima PoS sistema. U zavisnosti od toga kako se ključ čuva, načina enkripcije (šifrovanja) komunikacije između delova PoS sistema, ili nivoa zahtevane bezbenosti koriste se sledeći algoritmi:

Symmetric-key algoritmi - isti ključ se koristi za enkripciju i dekripciju podataka. Ovi algoritmi su brzi, ali manje „sigurni” i zahtevaju da su obe strane već razmenile ključeve ili lozinke, da bi mogle da dešifruju podatke. Primeri ovih algoritama su 3DES (*Triple Data Encryption*) i AES (*Advanced Encryption Standard poznatiji kao Rijndael*).

Asymmetric-key algoritmi - ovi algoritmi koriste dva ključa: jedan javni i jedan privatni. To znači da jedan ključ ne može biti korišćen i za enkripciju i za dekripciju podataka. Oba se ključa generišu istovremeno, privatni ostaje zaštićen pošto se koristi za dekripciju podataka, dok se javni objavljuje i koristi za enkripciju. Tipičan primer je osoba A piše poruku osobi B i enkripuje je sa javnim ključem osobe B. Po prijemu poruke osoba B koristi svoj privatni ključ za dekripciju poruke. Najčešći primeri PKI (public key infrastructure), kako se nazivaju asimetrični algoritmi za enkripciju su PGP/GPG (*Pretty Good Privacy*) i SSL/TLS (*Secure Socket Layer and Transport Layer Security*).

One-way hash algoritmi - koriste funkcije koje primaju informacije različite dužine i generišu izlaz fiksne dužine zavisno od ulaza. Prednost korišćenja ovakvih funkcija je

Iako preračunavanje i često se koriste za zaštitu lozinki, jer je uglavnom teško regenerisati regenerisati originalni unos na osnovu hash vrednosti.

5. ZAKLJUČAK

U cilju obezbeđenja što jednostavnije primene elektronskog plaćanja u maloprodajnim objektima potrebno je pored osnovnih servisa koje obezbeđuje poslovna banka kao davalac usluge korišćenja PoS terminala za bezgotovinsko plaćanje, implementirati i interfejs za integraciju PoS terminala u postojeći informacioni sistem. Ovakav interfejs omogućava jednostavniji rad sa karticama i veći stepen bezbednosti i kontrole. Direktnim povezivanjem PoS terminala i softvera za elektronsku kasu isključuje se mogućnost grešaka prilikom unosa iznosa za plaćanje, jer se on direktno preuzima iz softvera. Takođe iz PoS terminala se direktno preuzima status transakcije tako da ne može doći do pogrešnog tumačenja rezultata transakcije, što sve zajedno ceo proces čini bezbednijim i jeftinijim.

LITERATURA

- [1] Bogdanoski, B. (09.09.2014). *Asseco Protocol for connecting ECR with POS terminal*
- [2] Černenšek, M. *Serijska povezava pos terminala Ingeniko 5100 z napravu ECR*, Univerzitet v Mariboru Fakulteta za elektrotehniko, računarstvo in informatiko
- [3] PayEx (09.2014). *Specification of the ECR interface for PayEx terminals*
- [4] Veljović, A., Paunović L., (2014). *Elektronsko poslovanje*, FTN Čačak, Čačak
- [5] <http://poslovnainformatika.rs/elektronsko-poslovanje/distribuiranost-ep/> (16.03.2017)