Broj rada: 8(2010)3,181, 139 - 146

ULOGA PROCESORA PLAĆANJA U SERVISIRANJU ONLINE TRANSAKCIJA

Dr Marko Ranković*
EuroPlanet d.o.o, Beograd
Dr Vojkan Vasković
Beogradska Poslovna Škola

Uloga procesora u plaćanju može biti objašnjena jedino ukoliko se posmatra kao deo celine koju čine mnogi učesnici u sistemima plaćanja platnim karticama.

Procesor plaćanja ima važnu ulogu u realizaciji finansijskih online transakcija, od samog iniciranja transakcije, preko obrade, do dostavljanja odgovarajućeg odgovora na uređaj na kome je transakcija inicirana. Ovo procesor uključuje u kompletan životni ciklus transakcije. U zavisnosti od sistema kojim se transakcija realizuje (SMS, DMS) uloga procesora plaćanja se proširuje i na offline (batch) procesiranje transakcije u procesu sravnjivanja sa kartičnim organizacijama, odnosno drugim finansijskim institucijama.

Uloga procesora plaćanja zavisi od vrste uređaja na kojem je transakcija inicirana, od tipa transakcije (upit stanja, isplata, kupovina i sl.) i vrste transakcije (on-us, off-us transakcije).

Ključne reči: procesor plaćanja, online finansijske transakcije, modelovanje procesa obrade transakcija

ULOGA PROCESORA PLAĆANJA U SERVISIRANJU ONLINE TRANSAKCIJA

Procesor u servisiranju finansijske online učestvuje u sledećim procesima:

1. Sa ciljem uspešnog servisiranja online finansijske transakcije, procesor, pre svega, mora tu transakciju prilagoditi platformi za procesiranje – aplikaciji. Prilagođavanje poruke koja sa uređaja stiže predstavlja prevod u format transakcione poruke koja je u skladu sa logikom aplikacije za procesiranje. Pod uređajem se ne podrazumeva samo fizički uređaj sa kojeg transakcije može doći do procesora, već i mreža kartične organizacije ili nacionalnog switch-a. [2]
2. Nakon prevođenja poruke u odgovarajući format, obavlja se procesiranje transakcije. Rezultat procesiranja transakcije može biti:
   - validacija
   - validacija i autorizacija
   - prosleđivanje transakcije [15]

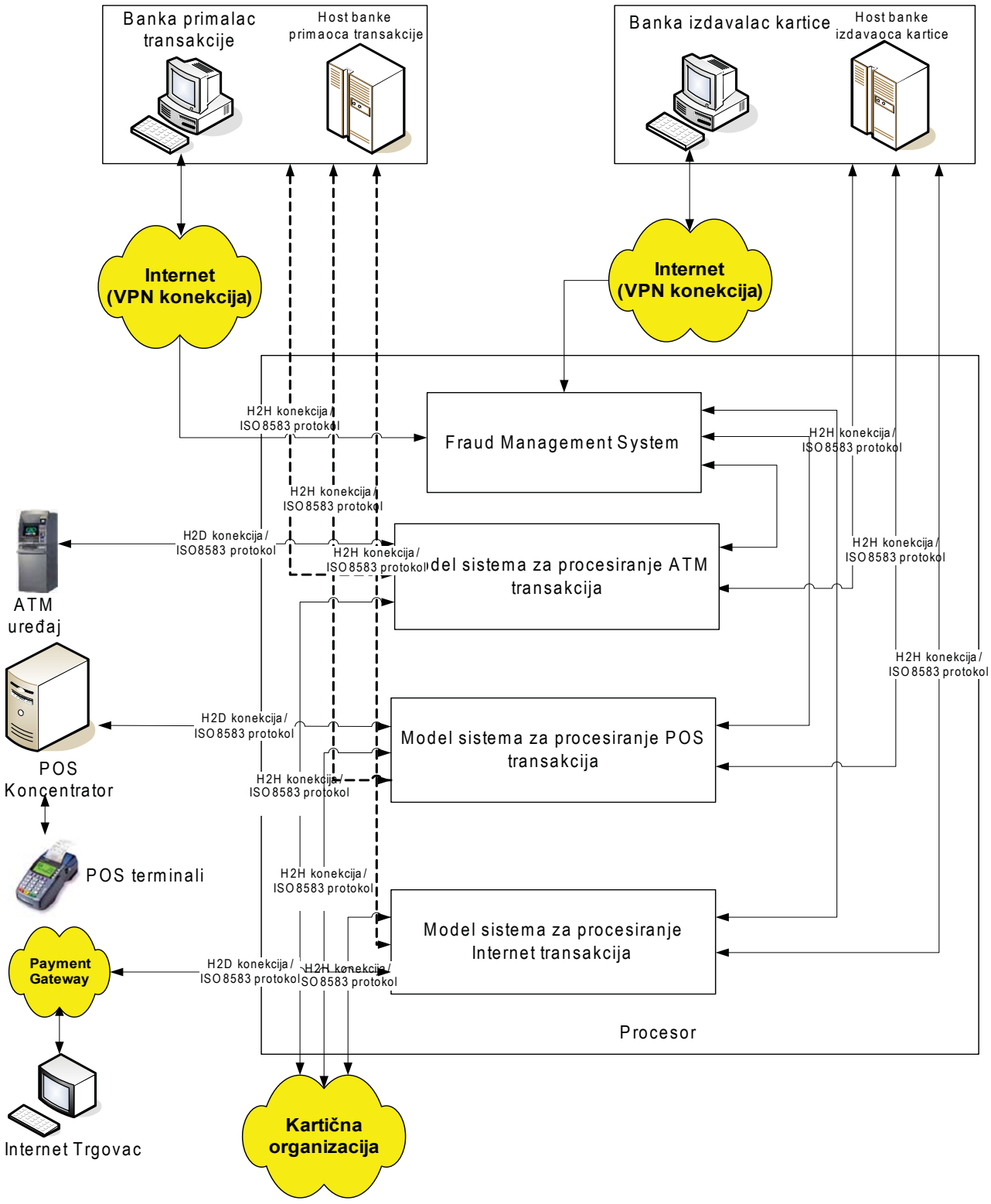
Proces validacije transakcije se odnosi na transakcije koje se obavljaju sa karticama banke izdavaoca kartica, a za koju procesor obavlja poslove procesiranja. Validacija se obavlja proverom određenih elemenata platne kartice. Elemente koje je potrebno proveriti propisuje PCI standard. [20]

Proces autorizacije se obavlja za transakcije koje se obavljaju sa karticama banke izdavaoca kartica, a za koju procesor obavlja poslove procesiranja. Autorizacija se obavlja proverom stanja na računu korisnika kartice i iznosa zahtevanih sredstava.

Prosleđivanje transakcije se realizuje u slučaju kada je na uređaju banke, za koju procesor obavlja procesiranje, obavljena transakcija sa karticom koja ne pripada toj banci. U ovom slučaju procesor priprema transakciju i prosleđuje je odgovarajućem entitetu. [6]

3. Prosleđivanje transakcionog odgovora odgovarajućem entitetu – uređaju ili kartičnoj organizaciji. Prosleđivanje odgovora podrazumeva da procesor mora da prilagodi format poruke koje predstavlja izlaz iz aplikacije zahtevima uređaja, kartičnih organizacija, nacionalnih switch-eva ili bankarskom back-office-u. Format poruka je u skladu sa standardom ISO 8583. [3]

* *EuroPlanet d.o.o., Makenzijeva 53/2, 11000 Beograd; mrankovic@eeft.com*



Slika 1. Model sistema za procesiranje elektronskih finansijskih transakcija sa procesorom u centralnoj ulozi

Svaki od ovih procesa je veoma kompleksan i sastoji se od brojnih podprocesa. Veoma važnu ulogu u procesima vezanim za implementaciju rešenja procesinga je planiranje, kao osnovna aktivnost menadžmenta. Planiranje toka rutiranja transakcije se realizuje u zavisnosti od odabranog poslovnog modela [17].

Svaka od veza procesora sa svakim entitetom je dvosmerna i veoma kompleksna. Svaka veza

podrazumeva posebne formate transakcionih poruka, posebne, a često dugotrajne i veoma skupe, postupke sertifikacije.

U definisanju same uloge procesora plaćanja u poslovnom modelu, važan je koncept outsourcinga. Procesori plaćanja jesu upravo uslužne kompanije koje pružaju usluge procesiranja finansijskih transakcije, kroz definisane modele outsourcinga. [8]

APLIKACIJA ZA PROCESIRANJE ONLINE TRANSAKCIJA

Savremene i visoko razvijene aplikacije za procesiranje u sebi sadrže integrisane elemente koji podržavaju procesiranje svih tipova transakcija, bez obzira na uređaj na kom su inicirane. [19]

Funkcionalne karakteristike aplikacija za procesiranje online transakcija

Aplikacija za procesiranje online finansijskih transakcija mora svojim funkcionalnim karakteristikama izaći u susret zahtevima klijenata i tržišta.[14] Aplikacija mora da obezbedi da svaka transakcija bude procesirana na odgovarajući, siguran način i da rezultat procesiranja bude prosleđen odgovarajućem entitetu.[9]

Osnovne funkcionalne karakteristike aplikacije za procesiranje online transakcija su:

- sigurnost
- pouzdanost
- fleksibilnost
- brzina
- skalabilnost

Aplikacija za procesiranje mora da podrži i sledeće osobine transakcione poruke:

- nedeljivost
- konzistentnost
- izolativnost
- trajnost [12]

Sigurnost

Aplikacija za procesiranje online finansijskih transakcija mora da odgovori zahtevima sigurnosti procesiranja transakcije, u delovima životnog ciklusa transakcije u kojima je uključena. Od trenutka kada primi transakciju, preko obrade, do dostavljanja rezultata procesiranja, aplikacija mora ispuni odgovarajuće sigurnosne kriterijume.[11]

Kriterijumi koji se odnose na sigurnost transakcije navedeni su u PCI DS (Payment Card Industry Data Security) standardu. [13]

PCI DS standard definiše stepen sigurnosti za određene elemente transakcione poruke (Tabela 1.)

Sistem za procesiranje mora da ispuni zahteve standarda u sledećim oblastima:

1. Sigurna mreža i mrežna infrastruktura
2. Zaštita osetljivih podataka (korisnik kartice, platna kartica)
3. Postojanje sistema za uočavanje i otklanjanje slabih tačaka
4. Primena restriktivnih mera kontrole pristupa
5. Kontinuiran nadzor i testiranje
6. Postojanje i dalji razvoj Politike sigurnosti podataka [20]

Tabela 1. Zahtevi PCI DS standarda o zaštiti elemenata transakcione poruke

	Data Element	Dozvoljeno čuvanje	Zahtevana zaštita
Podaci o korisniku platne kartice	Broj kartice (PAN)	Da	Da
	Ime korisnika kartice	Da	Da
	Servisni kod	Da	Da
	Datum važenja kartice	Da	Da
Poverljivi podaci za autentifikaciji	Podaci sa magnetne trake/čipa	Ne	N/A
	CAV2/CVC2/CVV2/CID	Ne	N/A
	PIN/PIN blok	Ne	N/A

Pouzdanost

Pouzdanost sistema za procesiranje predstavlja njegovu raspoloživost u toku određenog perioda. Korisnici platnih kartica i banke očekuju da sistem za procesiranje bude dostupan 24x7, 365 dana u godini. Mnogi faktori utiču da je, praktično, nemoguće ostvariti ovaj zahtev. To su najčešće objektivni razlozi, kao što je redovno održavanje sistema, nepredviđene situacije i sl. U praksi, raspoloživost sistema, na godišnjem nivou je od 99.5% do 99.9% [1]

Fleksibilnost

Aplikacija za procesiranje mora da bude veoma fleksibilna, kako bi mogla da odgovori zahtevima koji se pred nju postavljaju. Oštra konkurencija i ubrzani razvoj tržišta uslovljava brzo prilagođavanje novim zahtevima. Aplikacija mora da podrži uvođenje novih usluga kvalitetno i u kratkom vremenskom periodu, a da pri tom uslovi prilagođavanja ne budu skupi. Pored uvođenja novih usluga, aplikacije takođe mora podržati i prilagođavanje i svakom pojedinačnom zahtevu klijenta. [10]

Brzina

Brzina obrade transakcija predstavlja važnu karakteristiku aplikacije za procesiranje. Brzina procesiranja mora biti visoka, jer kartične organizacije definišu standardna vremena za realizaciju određenih transakcija. Sa druge strane, i procesoru je u interesu da obradi što više transakcija, jer svaka transakcija donosi novac. Potrebno je uskladiti performance sistema za procesiranje da bude u mogućnosti da obrađuje veliki broj transakcija za kratko vreme. [21]

Skalabilnost

Aplikacija za procesiranje mora da podrži i proširenje obima posla, odnosno da se prilagodi povećanom broju transakcija. [4]

Logičke celine aplikacije

Aplikacija za procesiranje online finansijskih transakcija je modularne arhitekture i sadrži sledeće logičke celine:

1. Komunikacioni modul
2. Kontrolni modul
3. Transakcioni modul
4. Security modul
5. Verifikaciono-validacioni moduli
6. Autorizacioni modul
7. Log modul

Aplikacija, u zavisnosti od organizacije arhitekture može imati i više od jednog modula. Moduli predstavljaju skup programa, koji se pozivaju na osnovu definisanih procedura. [10]

Komunikacioni modul

Komunikacioni modul predstavlja element kojim aplikacija komunicira sa spoljnim entitetima. Uloga komunikacionog modula je dvostruka. Ovaj modul, odstranjuje elemente komunikacionog protokola iz poruke koja u aplikaciju dolazi od nekog spoljnog entiteta. Modul izlaznim porukama iz aplikacije dodeljuje elemente komunikacionog protokola koji su neophodni za prenos. Komunikacioni moduli najčešće rade po TCP-IP protokolu. [18]

Komunikacioni modul dodeljuje jedinstveni broj svakoj transakciji, što olakšava praćenje transakcije kroz sistem. Jedinstveni broj transakcije omogućuje lakše istraživanje u slučaju problema.

Nakon dodeljivanja jedinstvenog broja, komunikacioni modul transakcionu poruku prosleđuje kontrolnom modulu.

Komunikacioni moduli se koriste, u suštini, predstavljaju interface aplikacije sa spoljnim svetom. Aplikacija preko komunikacionih modula komunicira sa:

- uređajima (ATM uređaj, POS terminal, Payment Gateway i sl.)
- kartičnim organizacijama (Visa, MasterCard, Dina, Diners, itd.)
- bankarskim back-office sistemima (FlexCube, Pexim Solutions, Arius, itd.)

Kontrolni modul

Kontrolni modul je arhitekturalno postavljen iza komunikacionih modula koji komuniciraju sa uređajima, odnosno mrežama. Uloga kontrolnog modula je da utvrdi tip uređaja na kojem je inicirana transakcija, da poruku prevede u odgovarajući format, koji je čitljiv za aplikaciju i da poruku prosledi sledećen modulu.

Kontrolni modul prevodi poruke koje u sistem dolaze u odgovarajući format, ali i formatira poruke koje iz sistema izlaze u formate koji od-

govaraju standardima entiteta kojima se poruka šalje. [10]

Transakcioni modul

Transakcioni modul prosleđuje transakcionu poruku na autorizaciju odgovarajućem entitetu.

Transakcioni modul na osnovu elemenata transakcione poruke (BIN) utvrđuje da li se radi o on-us ili off-us transakciji i na osnovu toga prosleđuje transakciju. Ukoliko su u pitanju on-us transakcije, ovaj modul transakcionu poruku prosleđuje security ili verifikaciono-validacionom modulu na dalje procesiranje. Ukoliko se radi o off-us transakciji, transakcioni modul poruku prosleđuje odgovarajućem kontrolnom modulu koji je dalje, preko komunikacionog modula, prosleđuje odgovarajućoj kartičnoj organizaciji.[10]

Security modul

Security modul ima ulogu validacije sigurnosnih elemenata, kao što su PIN, CVV, CVV2. Ovaj modul se najčešće realizuje kao HSM (Host Security Modul) uređaj, koji je integrisan u aplikaciju.

Verifikaciono-validacioni modul

Verifikaciono-validacioni modul verifikuje informacije o ispravnosti kartice, proverava limite korisnika kartice i nakon provere prosleđuje dalje transakcionu poruku. Ovaj modul verifikuje vrednosti CVV iz transakcione poruke, kao i datum važnosti kartice.

Autorizacioni modul

Autorizacioni modul verifikuje broj računa koje je prosleđen u transakcionoj poruci i autorizuje stanje na računu korisnika kartice. Da bi ovaj modul autorizovao transakciju potrebno je da stanja računa budu na host-u procesora.

Log modul

Ovaj modul upisuje sve poruke u log file. Čuvanje transakcionih poruka je definisano PCI DS standardom. Čuvanje poruka je izuzetno važno zbog istraživanja mogućih žalbi ili problema koji se mogu desiti.

ARHITEKTURA SISTEMA ZA PROCESIRANJE TRANSAKCIJA

Arhitektura sistema za procesiranje elektronskih finansijskih transakcija je modularno orijentisana. U zavisnosti vrste transakcije sistem koristi određene module kako bi servisirao finansijsku online transakciju. [16]

Komunikacioni modul 1 iz poruke, koja se komunikacionom linijom prenosi od uređaja (ATM, POS, Internet) do sistema za procesiranje, odstranjuje elemente komunikacionog protokola. Komunikacioni modul 1 prosleđuje transakcionu poruku Kontrolnom modulu 1.

Kontrolni modul 1 utvrđuje tip uređaja na kom je inicirana transakcija i prevodi je u odgovarajući format. Kontrolni modul 1 transakcionu poruku prosleđuje Transakcionom modulu i Kontrolnom modulu 1A.

Kontrolni modul 1A predstavlja interface između sistema za procesiranje i Fraud Management sistema. Ovaj modul prevodi poruku u format aplikacije Fraud Management sistema. Poruka se prosleđuje u bazu podataka FM sistema.

Sve transakcione poruke se smeštaju u bazu podataka. Fraud Processing sistem procesira transakcije, a na osnovu korisničkih i sistemskih pravila.

Operater banke pristupa FM GUI interface-u preko zaštićene Internet VPN veze i prati rezultate primene korisničkih i sistemskih pravila nad transakcijama. [7]

U slučaju da transakcija krši pravilo sa većom težinom, Fraud Management generiše odgovor kojim odbija transakciju i preko Kontrolnog modula 1A vraća odgovor na Kontrolni modul 1.

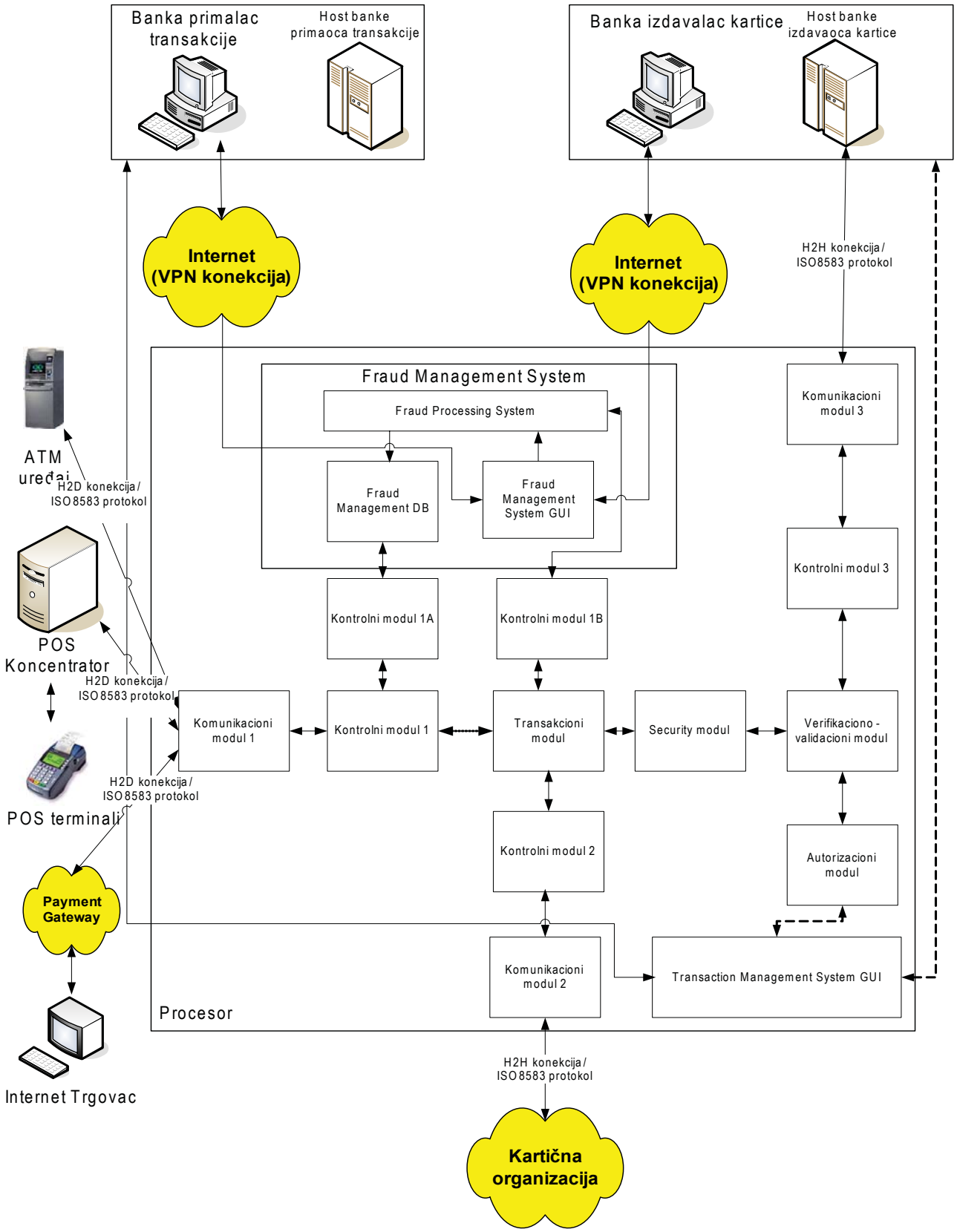
Ukoliko poruka ne krši pravila prosleđuje se preko Kontrolnog modula 1B na Transakcioni modul.

Transakcioni modul, na osnovu elemenata transakcione poruke, utvrđuje o kakvoj se vrsti transakcije radi (on-us; off-us) i utvrđuje kojem modulu je potrebno da prosledi poruku. Ako je transakcija inicirana sa platnom kartica banke čiji je i uređaj/medij koji je transakciju primio, a za koju procesor obavlja poslove procesiranja, Transakcioni modul poruku prosleđuje Security modulu.

Ukoliko je platna kartica ne pripada banci čiji je i uređaj, Transakcioni modul transakciju prosleđuje na Kontrolni modul 2, koji poruku prevodi u odgovarajući format po standardu ISO 8583 i poruku prosleđuje na Komunikacioni modul 2.

Security modul obavlja dekripciju posebno krip-

tovanih elemenata transakcione poruke (PIN block) i obavlja proveru PIN-a. [5] Ukoliko je korisnik uneo pogrešan PIN, ovaj modul odbija transakciju, sa odgovarajućim odgovorom. Ukoliko je PIN verifikovan, modul prosleđuje poruku Verifikaciono-validacionom modulu.



Slika 2. Model arhitekture sistema za procesiranje elektronskih finansijskih transakcija

Verifikaciono-validacioni modul obavlja validaciju ispravnosti kartice, da li je kartica važeća i, u zavisnosti od primenjenog poslovnog-tehničkog modela, transakcionu poruku prosleđuje Autorizacionom modulu ili Kontrolnom modulu 3.

Komunikacioni modul 2 poruci, koju mu je prosledio Kontrolni modul 2, dodaje elemente komunikacionog protokola i prevodi u odgovarajući format, pogodan za prenos.

Autorizacioni modul obavlja autorizaciju transakcije, odnosno potvrđuje da korisnik ima dovoljno sredstava na računu da realizuje transakciju ili u povratnoj poruci prosleđuje stanje na računu. Transakciona poruka se prosleđuje Autorizacionom modulu u slučaju da procesor u svom sistemu ima podatke o računima i stanjima računa. Ukoliko procesor ne poseduje podatke o računima i stanjima, transakciona poruka se prosleđuje na Kontrolni modul 3.

Kontrolni modul 3 transakcionu poruku prevodi u format koji odgovara zahtevima back-office-a banke i prosleđuje je na Komunikacioni modul 3.

Komunikacioni modul 3 transakcionoj poruci dodaje elemente komunikacionog protokola i prevodi je u format po TCP protokolu koji pogodan za prenos.

Komunikacioni moduli predstavljaju tačke sistema preko kojih transakcione poruke dolaza u sistem i iz sistema izlaze. Ove tačke predstavljaju interface-e sistema sa različitim entitetima koji se javljaju u procesu servisiranja finansijske online transakcije inicirane na različitim vrstama uređaja.

ZAKLJUČAK

Sagledavanje uloge procesora plaćanja u servisiranju online finansijskih transakcija predstavlja jasno definisanu ulogu procesora plaćanja u procesu servisiranja finansijskih transakcija, sistematizovan pregled modela sistema za procesiranje elektronskih finansijskih transakcija, sistematizovan prikaz aplikacije, funkcionalnosti aplikacija, kao i logičkih celina aplikacije za procesiranje online finansijskih transakcija. Rad prikazuje intergralni model sa procesorom plaćanja u centralnoj ulozi, što omogućuje sagledavanje te uloge, kao i uočavanje osnovnih funkcija procesora u sistemima plaćanja platnim karticama.

Model arhitekture sistema prikazuje osnovne celine aplikacije za procesiranje online finansijskih transakcija, što omogućava dalju raspravu o samoj logici aplikacije za procesiranje i programskim rešenjima pojedinih modula. U radu je prikazan tok transakcije, od modula do modula, i akcije koje se preduzimaju kao rezultati obrade transakcija. Model je sveobuhvatan i prikazuje sve učesnike u procesu.

Predloženi modeli omogućuju dalju nadgradnju funkcionalnosti koje se mogu ponuditi krajnjim korisnicima, kao što je implementacija sistema mobilnog bankarstva na predloženu infrastrukturu.

Primena modela arhitekture sistema za procesiranje elektronskih finansijskih transakcija omogućava smanjenje troškova u bankarskoj industriji, jer je primenjen Fraud Management sistem, koji obezbeđuje odbijanje transakcija za koje se sumnja da su zloupotrebe, a na osnovu prethodno definisanih parametara.

LITERATURA

1) Michael Gorham, Singh Nidhi, Electronic Exchanges: The Global Transformation from Pits to Bits, Academic Pr, 2009.
2) Marko Rankovic, “Istraživanje uloge procesora plaćanja u servisiranju online finansijskih transakcija“, doktorska disertacija, Beograd, FON, 2010.
3) Marko Rankovic, Tipovi i vrste krađa u sistemima plaćanja platnim karticama, InfoM, br. 28 – časopis za informacione tehnologije i multimedijalne sisteme, Beograd, 2008.
4) Mahmood Shah, Steve Clarke, E-Banking Management: Issues, Solutions, and Strategies, Information Science Publishing, 2009.
5) Paul Bocij, Dave Chaffey, Andrew Greasley, Simon Hickie, Business Information Systems: Technology, Development and Management, 3rd Edition, Financial Times Press, 2009.
6) Lloyd P. Blenman, Harold A. Black, Edward Kane, Banking and Capital Markets: New International Perspectives, World Scientific Publisher Company, 2009.
7) Timothy M. Virtue, Payment Card Industry Data Security Standard Handbook, Wiley, 2008.
8) Dominique Rambure, Alec Nacamuli, Payment Systems: From the Salt Mines to the Board Room (Studies in Banking and Finan-

cial Institutions), Macmillan, 2008

9) Ross McGill, Technology Management in Financial Services (Finance and Capital Markets), Macmillan, 2008
10) Martijn Groot, Managing Financial Information in the Trade Lifecycle: A Concise Atlas of Financial Instruments and Processes, Elsevier Scientific Publishing, 2008.
11) N. Subramani, V. Gamesan, D. Anbalagan, E-Commerce and E-Banking, Adroit Publishers, 2008.
12) Vadlamani Ravi, Advances in Banking Technology and Management: Impacts of ICT and CRM, Taylor and Francis, 2008
13) Dr Vojkan Vasković, Sistemi plaćanja u elektronskom poslovanju, FON, Beograd, 2007.
14) Miers, D., Strategic Chalenges of E-Commerce, 2003, http://www.enix.com
15) Armstrong, A., Hagel, J., The Real Value of Online Communities, Harvard Business Review, May - June, 2003
16) Hoffman, D. L., Novak, T.P., "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations," Project 2002 Working Paper No. 1, Owen Graduate School of Management, Vanderbilt University, 2002
17) Federal Financial Institutions Examination Council, E-Banking, 2003, http://www.occ.treas.gov/efiles/disk2/booklets/e_banking/e_banking.pdf
18) Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, 2004, http://www.ffiec.gov
19) Marko Rankovic, „Modeli i tehnike zaštite sistema plaćanja platnim karticama", magistarska teza, Beograd, 2008, FON

ROLE OF THE PAYMENT PROCESSOR IN THE ONLINE FINANCIAL TRANSACTIONS SERVICING

Role of the Payment Processor can be explained only if it is considered as part of the whole, which is composed of many participants of the payment card based systems.

The Payment Processor has an important role in the realization of the online financial transactions, from the transaction initiation, over processing, up to delivering the appropriate response to the device, from where transaction originated. This involves the processor into the all part of the transaction life cycle. Depending on the system, in which transaction is performed (SMS, DMS), role of the processor is extended to the offline transaction processing, through clearing and settlement processes, with other financial institutions.

The role of the Payment Processor also depends on the type of device, where the transaction is initiated, on the transaction type (balance inquiry, cash withdrawal, purchase, etc.) and the whether the transactions is on-us or off-us.

Keywords: payment processor, online financial transactions, transaction process modeling

Rad poslat na recenziju: 19.07.2010.
Rad spreman za objavu: 02.09.2010.