

# Plaćanje karticama

Goran Sladić

Katedra za informatiku, Fakultet tehničkih nauka, Novi Sad

2017.

# Platne kartice

- Vrste:
  - pre paid (telefonske kartice i sl.)
  - kreditne
  - debitne

# Prepaid kartice

- Zovu se još i *Electronic purse* i *Pay before*
- Uplati se unapred iznos i on se vezuje za karticu
  - nije vezan za račun u banci
- Primer:
  - telefonske kartice
  - elektronski novac (Visa prepaid)
  - menza

# Kreditne kartice

- Zovu se još i *Pay later*
- Predstavlja najstariji oblik kartica
- Istorija:
  - Koncept korišćenja kartica za plaćanje opisao još 1887 Edward Bellamy
  - 1920ih koriste se u SAD za prodaju goriva na pumpama
  - Koncept da kupci jednom karticom mogu plaćati različite stvari uveden je 1950 od strane osnivača Diner Club-a
- Inicijalno nisu bile elektronski podržane
  - bile su paper-based

# Učesnici kod plaćanja karticama

- Učesnici u procesu kupovine korišćenjem kartice:
  - cardholder – klijent, korisnik kartice
  - Issuer – izdavalac (izdaje karticu)
  - Merchant – trgovac, akceptant
  - Acquirer – prihvatilac kartice (instalira POS terminal ili ATM)
    - Payment processor – firma koja obavlja posao autorizacije, obrade i razmene podataka
  - Asocijacija – entitet koji koordinira sve transakcije

# Credit Card Association

- Asocijacije koje omogućuju rad sa kreditnim karticama i ne bave direktno mušterijama i trgovcima
- Učesnici:
  - Credit Card Association – udruženje banaka i kompanija koje posreduju u radu
    - Visa, MasterCard, American Express, Diners Club
  - Issuer – onaj ko je izdao karticu mušteriji
    - može da bude banka ili neka kompanija
  - Acquirer – onaj kod koga se trgovci registruju
    - može da bude banka ili specijalizovana kompanija

## Credit Card Association II

- Prihode ostvaruju od:
  - članarine
  - procenta od transakcija
- Upravni odbor (Board of directors) upravlja radom asocijacije
- Jedna banka može biti član u više asocijacija
- Funkcije asocijacije:
  - izdavanje regulativa
  - procesiranje transakcija i iniciranje clearing & settlement procesa
  - razvoj
  - promocija
  - bezbednost
  - STIP (STand In Processing) – obavlja autorizaciju transakcije (ako je Issuer nedostupan), po unapred definisanim parametrima

# Issuer

- Banke ili kompanije koje izdaju kartice
- Upravni odbor (Board of directors) upravlja radom asocijacije
- Jedna banka može biti član u više asocijacija
- Zaradu imaju od:
  - procenta koji uzimaju trgovcima koji su primili njihovu karticu (od oko 2%, uzimaju 1,4%)
  - kamate na kredit korisnicima kartice



# Acquirer

- Banka ili kompanija koja se bavi tehničkim i finansijskim elementima rada
  - instalacija terminala
  - obezbeđivanje servisa za autorizaciju na osnovu podataka iz kartice
  - logovanje transakcija i slanje izveštaja trgovcima
  - transfer sredstava trgovcima na dnevnoj bazi
  - rešavanje problema
- Zaradu imaju od:
  - procenta koji uzimaju trgovcima koji su primili njihovu karticu (od oko 2%, uzimaju 0,6%)

# Paper-based kreditne kartice I

- Mušterija daje kreditnu karticu trgovcu
- Opciona provera telefonom
  - provera da li je na crnoj listi (ovo može biti odštampan spisak koji se isporučuje trgovcima)
- Pravljanje sales voucher-a
  - koristi se imprinter
  - sadrži broj kreditne kartice, iznos, datum i opis
  - mušterija potpisuje vaučer
- Kupovina se završava
- Na kraju radnog dana, trgovac skuplja sve sales voucher-e i predaje ih acquiring banci
- Acquirer inicira clearing & settlement koristeći automatizovan sistem
- Novac se skida sa računa mušterije i prebacuje na račun acquirer-a
- Acquirer prebacuje novac svim registrovanim trgovcima

## Paper-based kreditne kartice II

- Gde je razlika u odnosu na čekove?
  - novac se troši unapred, odnosno na kredit
  - postoji limit – ne može svako da dobije kreditnu karticu
    - limit se u papirnoj verziji nije mogao automatski proveravati
  - početkom meseca stiže račun sa spiskom i ukupnom sumom
    - račun ne mora da se isplati u celini
    - ako se isplati neki deo (postoji definisan minimum), to je revolving kreditna kartica

# Debitne kartice

- Zovu se još i *Pay now*
- Kartica je vezana za račun i ne može se potrošiti više nego što ima na računu
- Zahteva real time autorizaciju

# Procedura

- Autentifikacija kartice (magnetne i čip)
  - Static Data Authentication (SDA)
  - Dynamic Data Authentication (DDA)
- Algoritam autentifikacije
  - simetrično kriptovanje
  - asimetrično kriptovanje
- Verifikacija vlasnika
- Autorizacija transakcije
  - off-line – u terminalu
  - on-line – na serveru izdavača kartice (Issuer Host – IH)
    - Single Message System (SMS)
    - Dual Message System (DMS)
- Clearing & settlement
- Isplata gotovine sa ATM-a/predaja-isporuka sredstava

# Autentifikacija I

- Proces autentifikacije kartice – utvrđivanje da li je kartica ispravna sa stanovišta bezbednosti, odnosno da li su podaci na kartici validni
  - jako bitno kod kupovine preko Interneta, pošto nema direktnog kontakta između trgovca i mušterije, a koristi se samo PAN
- Vrste autentifikacije kartica:
  - Static Data Authentication (SDA)
    - kod magnetnih i kod smart kartica
    - verifikacija integriteta podataka na kartici – ekvivalent čeksuma, odn. potpisa
    - ne sprečava falsifikovanje
  - Dynamic Data Authentication (DDA)
    - challenge/response mehanizam
    - kod smart kartica

## Autentifikacija II

- Mesto autentifikacije kartica
  - terminal - off-line
  - IH (Issuer Host) – on-line
- Slanje PIN-a na proveru (kod smart kartica)
  - SDA autentifikacije, PIN se ne šifruje dok se šalje kartici
  - DDA autentifikacije, PIN se šifruje dok se šalje kartici

# Verifikacija vlasnika

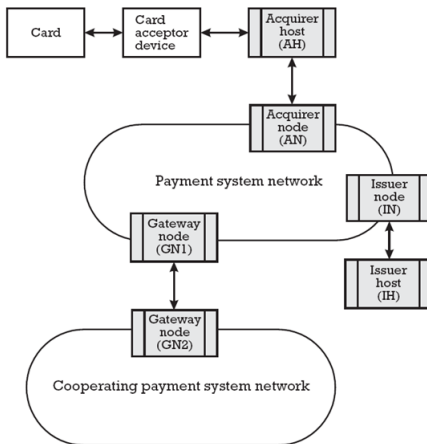
- Vrste
  - PIN
  - potpis
  - ništa



# Autorizacija transakcije

- Zasniva se na razmeni finansijskih poruka između učesnika
- Učesnici:
  - terminal (Card Acceptor Device)
  - AH (Acquirer Host)
  - AN (Acquirer Node)
  - IN (Issuer Node)
  - IH (Issuer Host)
  - Asocijacija - Payment System Network
  - Gateway Node

# Mreža



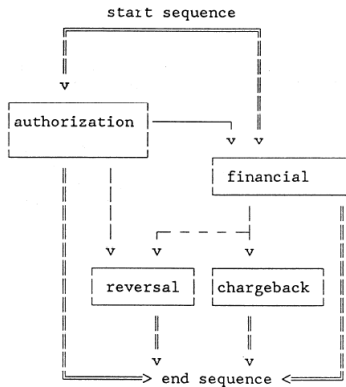
# Finansijske poruke

- ISO 8583
- Struktura:
  - Identifikator tipa poruke
    - četiri cifre
  - bitmapa
    - indeksi polja u poruci, 64-bitna bitmapa
  - niz elemenata

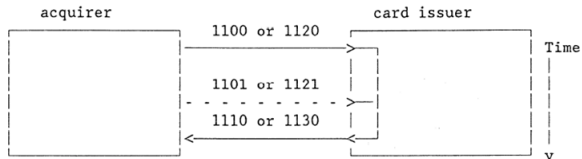
## ISO 8583 – vrste poruka

- Autorizacija transakcije
- Finansijska transakcija
- File action
- Reversal - poništavanje
- Chargeback – povraćaj novca nakon uspešno okončane transakcije (neisporučena roba, oštećena roba, itd.)
- Acquirer reconciliation transactions – poravnanje stanja acquirer-a
- Card issuer reconciliation transactions – poravnanje stanja issuer-a
- Administrative transactions
- Acquirer fee collection transactions – prikupljanje provizije za acquirer-a
- Card issuer fee collection transactions – prikupljanje provizije za issuer-a
- Network management transactions

# Tok poruka

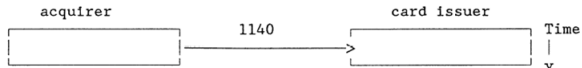


# Tok poruka - Autorizacija transakcije



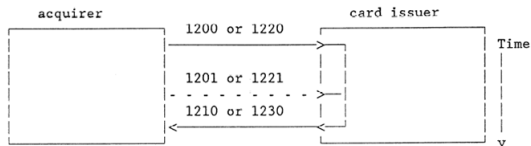
1100/1101 authorization request/authorization request repeat  
 1110 authorization request response

1120/1121 authorization advice/authorization advice repeat  
 1130 authorization advice response



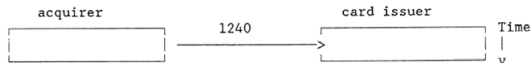
1140 authorization notification

# Tok poruka - Finansijska transakcija



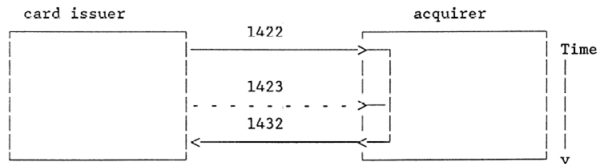
1200/1201 financial request/financial request repeat  
 1210 financial request response

1220/1221 financial advice/financial advice repeat  
 1230 financial advice response

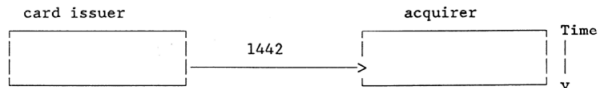


1240 financial notification

# Tok poruka - Chargeback transaction



1422/1423 chargeback advice/chargeback advice repeat  
1432 chargeback advice response



1442 chargeback notification



# ISO 8583 identifikator tipa poruke I

- Prva cifra:
  - 0 – rezervisano
  - 1 – tekuća (1993) verzija poruke
  - 2-7 – rezervisano
  - 8 – rezervisano za domaću upotrebu
  - 9 – rezervisano za privatnu upotrebu
- Druga cifra:
  - 0 – rezervisano
  - 1 – authorization (samo rezervišne sredstva)
  - 2 – financial (direktno skida sredstva sa računa vlasnika)
  - 3 – file action messages (za upravljanje crnim listama – dodavanje, brisanje, itd.)
  - 4 – reversal/chargeback
  - 5-8 – reconciliation, administrative, fee collection, network management

# ISO 8583 identifikator tipa poruke II

- Treća cifra:
  - 0 – request
  - 1 – response
  - 2 – informacija sa advice porukom; odgovor je obavezan
  - 3 – advice response message
  - 4 – notification message; ne zahteva se odgovor
- Četvrta cifra:
  - 0 – acquirer inicira transakciju
  - 1 – acquirer inicira ponovljenu transakciju
  - 2 – issuer inicira transakciju
  - 3 – issuer inicira ponovljenu transakciju
  - 4, 5 – neko drugi inicira transakciju/ponovljenu transakciju

# ISO 8583 bitmapa

- 64-bitno polje (i opcionalno/sekundarno još jedno 64-bitno polje)
- Svaki bit označava prisustvo/odsustvo asociiranog polja
  - svaki bit je dodeljen jednom polju
- Primarno bit polje je uvek prisutno

## ISO 8583 bitmapa - Primer

- Bit 1 - da li postoji sekundarna bit mapa
- Bit 2 - PAN pristutan
- Bit 3 - processing code
- Bit 4 - iznos transakcije
- ...

# ISO 8583 niz polja

- Svako polje je zadate širine
- Na osnovu bit-mape, parser zna koja polja postoje, i na osnovu širine, zna gde je sledeće polje
- Ako je polje varijabilne širine, uvek ide prvo broj bajtova, pa sam sadržaj
- Primer PAN polje
  - **19**1234500000543210000

# Primer request I

12007014059808c08000191234500000543210000000000  
00000000000020708052044192610000054  
2001506000000001123456789012cheefpos3101060434700978

# Primer request II

```
#-----+-----+-----+-----+
|field| Value          | bold | | green |
|      | Description     | default | |=additional |=full |
+-----+-----+-----+-----+
| MTI | 1200
|      | Message type - financial request
| 000 | 7014059808c08000
|      | Primary Bit Maps
|      |=011100000000101000000010110011000000010001100000010000000000000000
| 002 | 1234500000543210000
|      | primary account number
| 003 | 000000
|      | processing code
|      |=00-Goods and service
|      |=00-Default - unspecified - debits,inquiries, "from" account
|      |=00-Default - unspecified - credits and the "to" account
| 004 | 0000000000002
|      | amount, transaction
| 012 | 070805204419
|      | YYMMDDhhmmss - date and time, local transaction
| 014 | 2610
|      | YYMM - date, expiration
| 022 | 0000 54
|      | point of service data code
|      |=0-unknown
|      |=0-no electronic authentication
|      |=0-none
|      |=0-no terminal used
|      |= -
|      |= -
|      |= -
|      |=5-manual signature verification
|      |=4-by merchant
|      |= -
|      |= -
|      |= -
```

# Primer request III

```

| 024 | 200
|      | function code
|      | =200-original financial request/advice
| 025 | 1506
|      | message reason code
|      | =1506-on line forced by card acceptor
| 028 | 000000
|      | YYMMDD - date, reconciliation
| 029 | 001
|      | reconciliation indicator
| 037 | 123456789012
|      | retrieval reference number
| 041 | cheefpos
|      | card acceptor terminal identification
| 042 | 3101060434700
|      | card acceptor identification code
| 049 | 978
|      | currency code, transaction
|      | =euro

```

+-----+



# Primer response I

1210700000000e8080001912345000005432100000000000  
0000000000002123456789012118cheefpos978

34 / 58

# Tokovi poruka

- Postoji više scenarija:
  - off-line transaction authorization
  - on-line transaction authorization
- Postoji više načina razmene:
  - Dual Message System
  - Single Message System
- Učesnici:
  - POS terminal/ATM
  - AH (Acquirer Host)
  - IH (Issuer Host)
  - Asocijacija

# Dual Message System I

- Autorizacija iz dva koraka
  - autorizaciona poruka kojom se rezervišu sredstva
  - finansijska poruka kojom se sredstva skidaju sa računa
- Vrste autorizacije:
  - on-line
    - AH šalje do IH Authorization Request Message (1100)
    - IH šalje do AH Authorization Request Response Message (1110) sa potvrdom transakcije ili odbijanjem (sredstva se samo rezervišu)
  - off-line
    - autorizaciju transakcije obavlja terminal
    - nema saobraćaja između AH i IH u ovoj fazi, već se prilikom clearing-a šalju dve poruke (Authorization Advice Message, pa zatim Financial Notification Message)

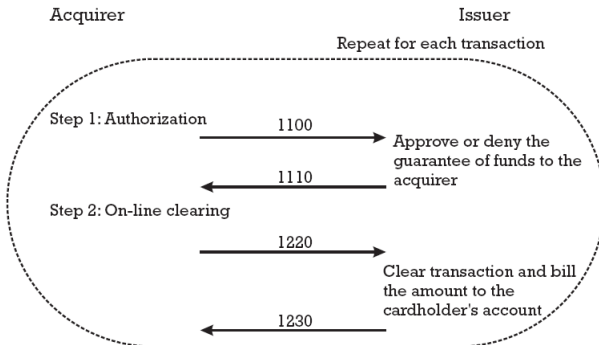
## Dual Message System II

- Alternative clearing-a kada se obavi on-line autorizacija:
  - on-line clearing
    - AH šalje do IH Financial Advice Message (1220) sa zahtevom da se sa računa vlasnika skinu rezervisana sredstva
    - IH šalje do AH potvrdu u vidu Financial Advice Response Message (1230)
    - sredstva sa računa vlasnika su skinuta i prebačena na račun Issuer-a
  - off-line clearing
    - AH po prispeću Authorization Request Response Message (1110) slaže Financial Notification Message (1240) u clearing batch fajl
    - periodično (kada trgovac inicira završetak rada/jednom dnevno/itd.) clearing batch fajl se šalje do IH koji skida sredstva sa računa svih vlasnika
    - sredstva sa računa svih vlasnika su skinuta i prebačena na račun Issuer-a

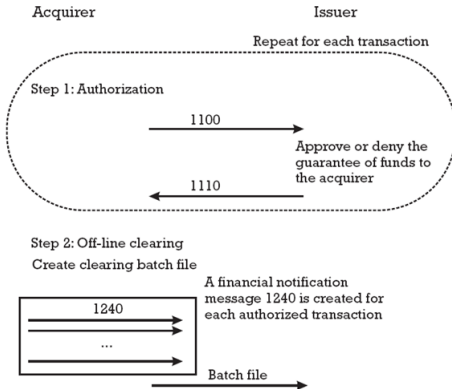
# Dual Message System III

- Kada se obavi off-line autorizacija, sledi off-line clearing:
  - kada trgovac inicira završetak rada (npr. jednom dnevno)
    - podaci o svim transakcijama se šalju od POS terminala do AH
    - AH za svaku transakciju šalje do IH Authorization Advice Message (1120)
    - IH šalje do AH potvrdu ili odbijanje preko Authorization Advice Response Message (1130)
    - formira se clearing batch fajl koji se sastoji iz Financial Notification Message (1240) za sve prihvaćene transakcije
    - AH šalje clearing batch fajl do IH, a ovaj za svaku poruku skine novac sa računa vlasnika i prebaci na svoj račun

# On-line transaction authorization, on-line clearing

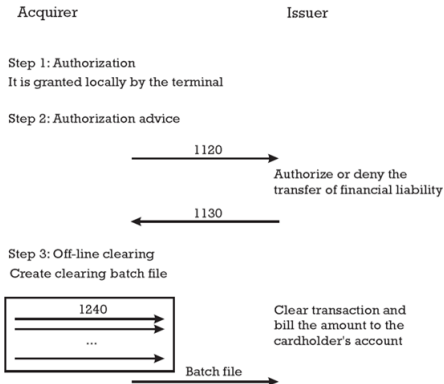


# On-line transaction authorization, off-line clearing





# Off-line transaction authorization, off-line clearing



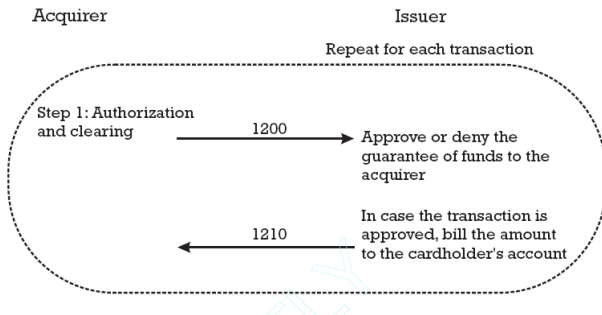
# Single Message System I

- Iznos se momentalno skida sa računa jednom porukom
- On-line transaction authorization, on-line clearing:
  - AH šalje do IH Financial Request Message (1200)
  - IH šalje do AH Financial Request Response Message (1210) sa potvrdom transakcije ili odbijanjem
    - sredstva su skinuta sa računa vlasnika i prebačena na račun Issuer-a

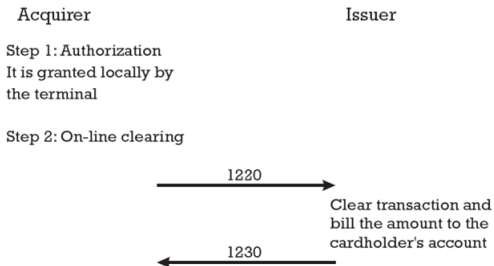
## Single Message System II

- Off-line transaction authorization, on-line clearing:
  - autorizaciju transakcije obavlja terminal
  - kada trgovac inicira završetak rada/periodično/itd.
    - podaci o svim transakcijama se šalju od POS terminala do AH
    - za svaku transakciju, AH šalje do IH Financial Advice Message (1220)
    - IH šalje do AH potvrdu u vidu Financial Advice Response Message (1230)
    - skida sredstva sa računa vlasnika i prebacuje na račun Issuer-a

# On-line transaction authorization, on-line clearing



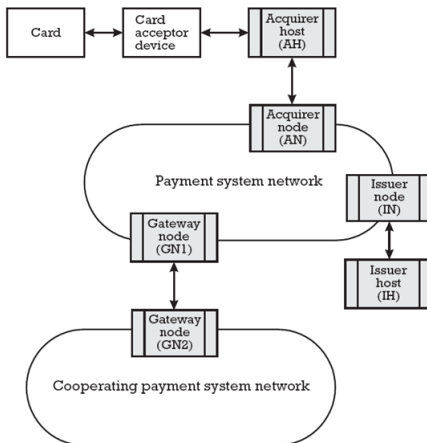
# Off-line transaction authorization, on-line clearing



# On-line autorizacija transakcije

- Bilo da je DMS ili SMS, pruža sledeće povoljnosti:
  - pošto IH odobrava transakciju, korisnik je sigurniji od zloupotreba
    - kod off-line, nema komunikacije između trgovca i IH – ukradena kartica sa promenjenom opcijom za CVM (cardholder verification method) na “samo potpis” ili na “Yes card” može da prevari terminal (lopov ne mora da zna PIN)
    - CVM kod nekih karitca nije obuhvaćen digitalnim potpisom!
  - pošto Asocijacija garantuje isplate za sve on-line autorizacije, trgovac je zaštićen od zloupotrebe

# Mreža



# On-line autorizacija transakcije - Scenario I

- Po okončanoj autentifikaciji i verifikaciji klijenta terminal šalje zahtev do AH
- AH proverava da li je zahtev kompletan i korektan
- AH šalje zahtev do Asocijacije
- Asocijacija proverava da li je kartica iz sistema asocijacije ili iz neke druge
  - ako je iz sistema, na osnovu Issuer Identification Number (IIN) prosleđuje poruku do IN
  - ako nije iz sistema, poruka se šalje preko Gateway Node1 do druge asocijacije
    - tu se na osnovu IIN poruka prosleđuje do IH



## On-line autorizacija transakcije - Scenario II

- IH proverava kompletnost i korektnost prispele poruke
  - proverava se validnost PAN-a i datum isteka kartice
  - ako je i PIN prosleđen, proverava se
  - proverava sredstava
    - ako je debitna kartica, proverava se da li ima sredstava
    - ako je kreditna kartica, proverava se da li je premašen limit
- svi odgovori od IH sadrže odgovarajući Reference Number da bi ih povezali sa zahtevima

# Clearing and Settlement

- Clearing – proces u kojem Acquirer obaveštava Issuer-e o transakcijama koje su inicirali vlasnici kartica
  - na osnovu ovih informacija, Issuer skida sredstva sa računa vlasnika
- Settlement – proces u kojem se poravnavaju računi Issuer-a i Acquirer-a
  - na osnovu clearing informacija, sredstva se prebacuju sa računa Issuer-a na račune Acquirer-a

# Clearing

- Acquirer prikuplja sve transakcije i šalje ih u Asocijaciju
- Asocijacija sortira transakcije po Issuer-ima i šalje im clearing batch poruke
  - to radi na osnovu IIN (Issuer Identification Number)
  - Issuer-i na osnovu pristiglih clearing poruka znaju koliko sredstava kojem vlasniku da skinu
    - poruke u batch fajlu su sortirane po PAN-ovima
    - pošto iznosi iz transakcija mogu da budu u različitim valutama, radi se zamena u billing valutu koju je definisao Issuer
    - ako je debitna kartica, sredstva se uzimaju direktno sa računa
    - ako je kreditna kartica, sredstva se zapisuju u specijalni račun, povezan sa kreditnom karticom (ovaj račun ide u minus)

# Settlement I

- Učesnici:
  - Acquier
  - Issuer
  - Clearing house
  - Trgovac

# Settlement II

- Nakon što je clearing urađen, radi se settlement
- Issuer-i i Acquirer-i imaju otvorene račune kod Clearing house
- Asocijacija po prijemu svih transakcija, osim generisanja clearing batch fajla, radi i multilateralni neto
  - sračunava koliko koji Issuer duguje kojem Acquirer-u, u totalu
  - šalje naloge Clearing house-u da se taj novac prebaci sa računa Issuer-a na račun Acquirer-a
  - iznosi mogu biti u različitim valutama, pa se za svaku transakciju razmenjuju iz valute na mestu kupovine u valutu za settlement (koju je ugovorio Issuer), po kursu koji diktira Clearing house
  - po prebacivanju sredstava, Asocijacija obaveštava Issuer-a i Acquirer-a o iznosima koji su prebačeni
- Acquirer prebacuje primljena sredstva na pojedinačne račune trgovaca

## Veoma pojednostavljen primer

- Stranac u radnji kupuje robu u vrednosti od 1000 din
- Njegov Issuer je u Nemačkoj i radi sa evrima
- Novac se prilikom clearing-a konvertuje u 10 EUR
  - Issuer skida 10 EUR sa računa vlasnika
- Issuer uzima 1,4% od 10 EUR, odn. 0,14 EUR za sebe
- Novac koji se prosleđuje prilikom settlement-a od Issuer-a do Acquirer-a je 9,86 EUR
- Acquirer-u je stiglo 9,86 EUR, koje on preračunava u dinare: 788,8 dinara
  - Provera:  $800 - 1,4\%$ , odn.  $800 - 11,2 = 788,8$
- Acquirer od 788,8 dinara uzima za sebe (0,6% od 800 dinara, a to je) 4,8 dinara i prebacuje trgovcu 784 dinara
- Iako je ilegalno, neki trgovci
  - naplaćuju dodatno prilikom kupovine karticom
  - daju popust ako se kupuje za gotovinu

# DINA

- Učesnici:
  - NBS
  - Nacionalni Centar za Platne Kartice (NCPK)
  - Switch sistem
  - Issuer (Izdavalac)
  - Acquirer (Prihvatilac)
  - Vlasnik kartice

# NBS

- Svi učesnici imaju otvorene račune u NBS
- NCPK je ovlašćen od strane učesnika da raspolaže računima učesnika kod NBS
- NCPK šalje RTGS poruke za prenos sredstava prilikom računanja multilateralne neto pozicije



# NCPK

- NCPK je ovlašćen od strane banaka da prebacuje sredstva sa računa učesnika, koji su otvoreni pri NBS
- Jednom dnevno radi se multilateralni neto obračun (multilateral netting) gde se sračunava neto pozicija učesnika
  - ako je issuer, on je u minusu, NCPK prebacuje sredstva sa issuer-ovog računa na svoj
  - ako je acquirer, on je u plusu, NCPK prebacuje sredstva sa svog računa na acquirer-ov
- Naplaćuje usluge
- Koristi se DMS za POS terminale, a SMS za bankomate

# Switch sistem

- Povezuje učesnike
- Rutira poruke
- Formira i održava različite datoteke
- Stand-in autorizacija
  - kada je issuer nedostupan, Switch sistem obavlja autorizaciju transakcije na osnovu datoteke sa stanjima ili na osnovu zadatih parametara
- Clearing svih transakcija