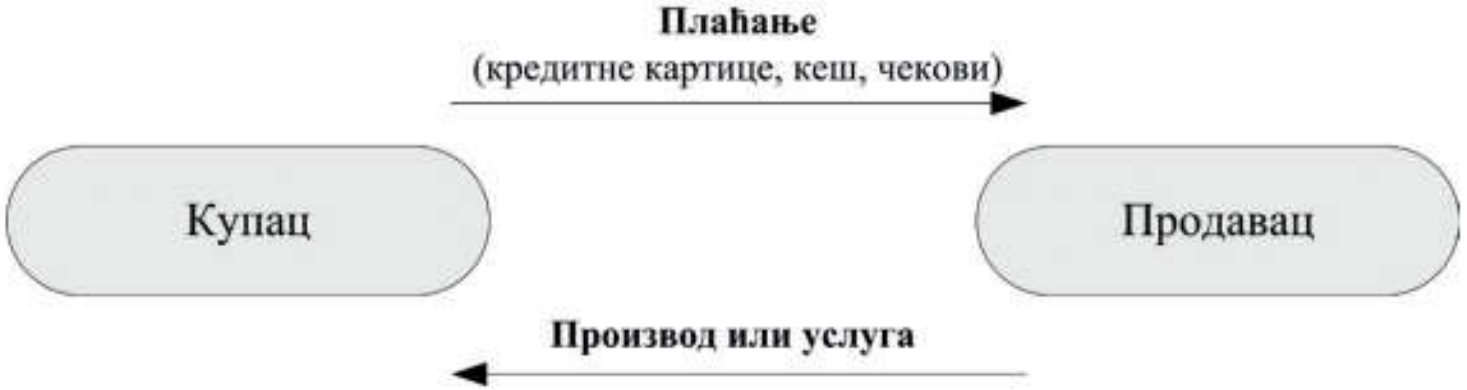

Sistemi elektronskog
plaćanja

Sistemi elektronskog plaćanja

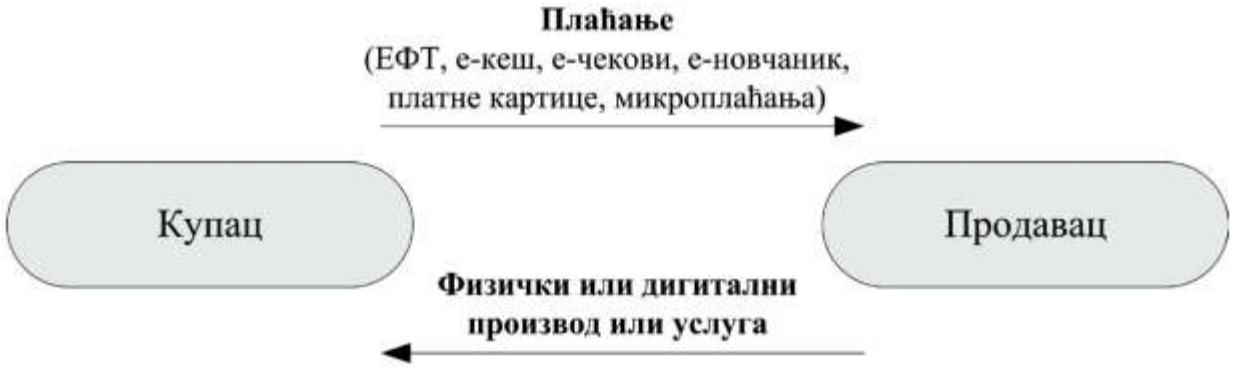
- Ekonomske posledice elektronskog novca
- Online i offline plaćanja elektronskim novcem
- Mikro plaćanja
- Mehanizmi i instrumenti elektronskog plaćanja
- Inteligentne kartice

Tradicionalni sistem plaćanja

- Kupac vidi proizvod, donosi odluku o kupovini i nakon toga plaća kešom, čekom ili karticom.



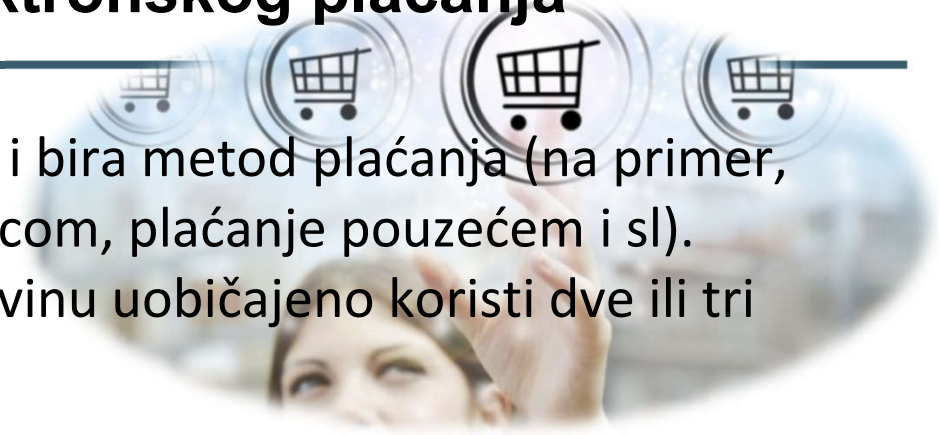
Elektronski sistem plaćanja



Modeli i mehanizmi plaćanja na Internetu

- U odnosu na tradicionalne modele plaćanja, u sistemima elektronskog plaćanja potrebno je veće poverenje i prihvatanje pravila.
- Kupac ne može uživo da vidi proizvod u trenutku kupovine, a metodi plaćanja se realizuju elektronskim putem.
- Glavni cilj sistema elektronskog plaćanja je povećanje:
  - efikasnosti,
  - isplativosti,
  - poboljšana sigurnost i
  - jednostavnost korišćenja.

Ključne uloge u sistemima elektronskog plaćanja



- **Kupac**. Kupac inicira proces plaćanja i bira metod plaćanja (na primer, PayPal, Visa kartica, plaćanje uplatnicom, plaćanje pouzećem i sl). Prosečan kupac za elektronsku kupovinu uobičajeno koristi dve ili tri metode elektronskog plaćanja.

- **Prodavac**. Prodavac na svom veb-sajtu može omogućiti više metoda i sistema plaćanja, a kupac bira koji od dostupnih metoda će koristiti. Veći broj raspoloživih sistema plaćanja u elektronskoj prodavnici trebalo bi da privuče više kupaca.

- **Procesor plaćanja.** Procesor plaćanja je posrednik koji omogućava prodavcima da u elektronskoj trgovini naplaćuju platnim karticama. Najpoznatiji globalni procesori plaćanja su: **PayPal, Verisign, 2Checkout, Worldpay** i drugi. Veći broj procesora plaćanja posluje na lokalnim tržištima.

Modeli i mehanizmi plaćanja na Internetu

- U početnim fazama razvoja sistema plaćanja na Internetu nije bilo moguće realizovati kompletne transakcije, već su primenjivani hibridni modeli plaćanja.

- Primeri hibridnih mehanizama su plaćanje pouzećem, kombinacija telefona i Interneta, plaćanje putem opštih uplatnica nakon naručivanja putem Interneta i slično.

- Danas postoji veliki broj različitih podela

  kada su u pitanju mehanizmi elektronskog plaćanja.

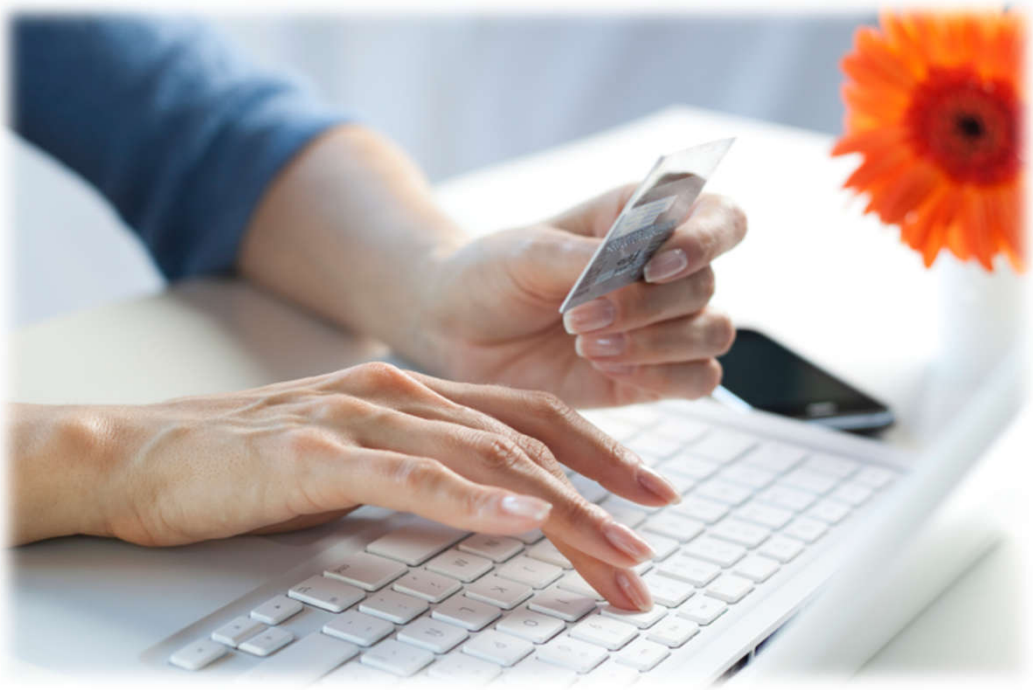
  Može se uočiti da se modeli i metode plaćanja tokom

  vremena menjaju, tako da je i klasifikacija ovih modela i metoda

  promenljiva.

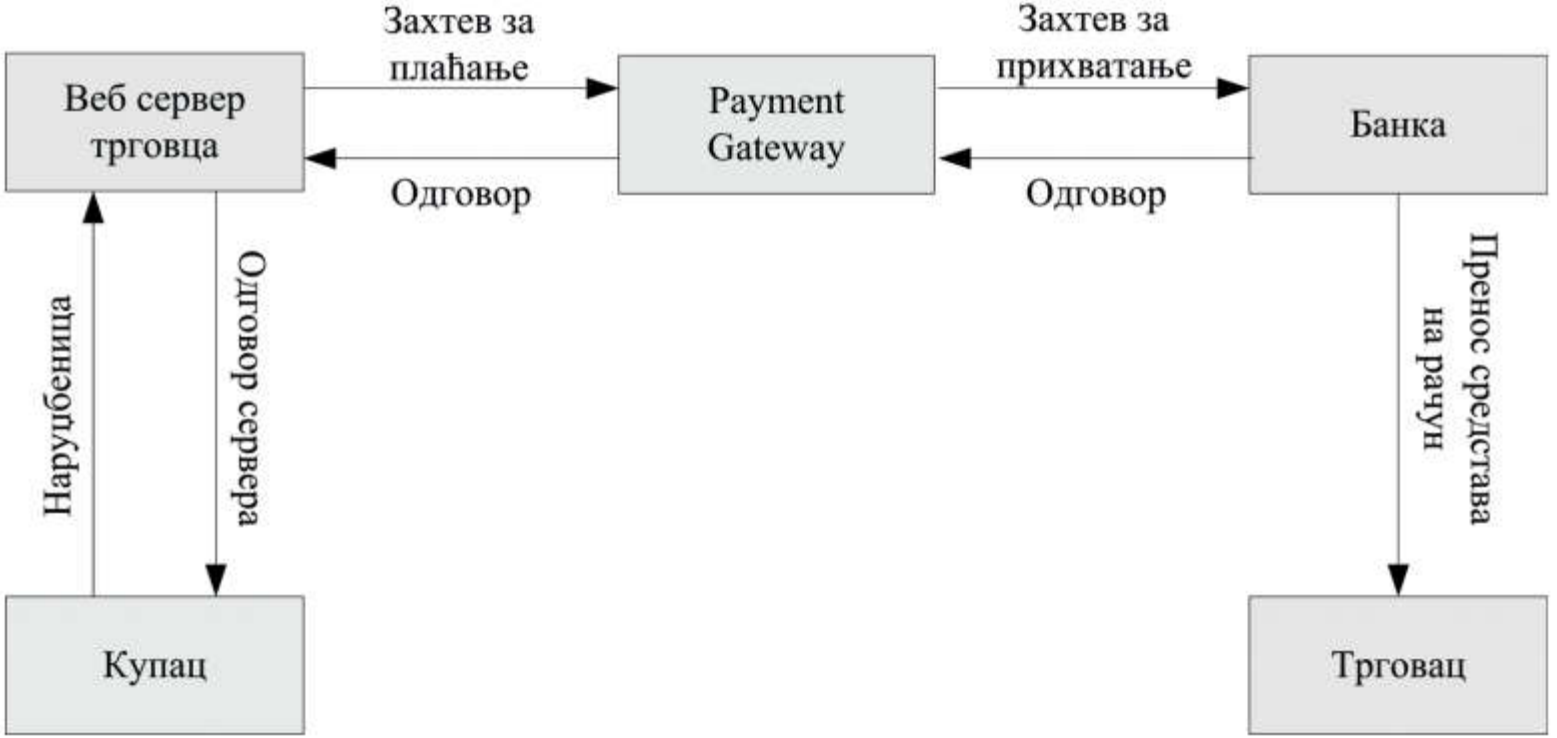
Modeli i mehanizmi plaćanja na Internetu

- Kao najčešće korišćeni sistemi plaćanja na Internetu mogu se izdvojiti:
  - platne kartice;
  - elektronski čekovi;
  - elektronski keš;
  - elektronski novčanici;
  - P2P plaćanja;
  - plaćanja vaučerima;
  - mikroplaćanja;
  - mobilna plaćanja;
  - sistemi zasnovani na zlatu;
  - kriptovalute.



Platne kartice

- Upotreba platnih kartica za plaćanja na Internetu zasniva se na proširenju funkcionalnosti platnih kartica koje se koriste za plaćanja na fizičkim mestima prodaje.
- Za plaćanja na Internetu mogu se koristiti svi tipovi platnih kartica.
- Bez obzira na tip kartice, proces realizacije plaćanja je sličan.

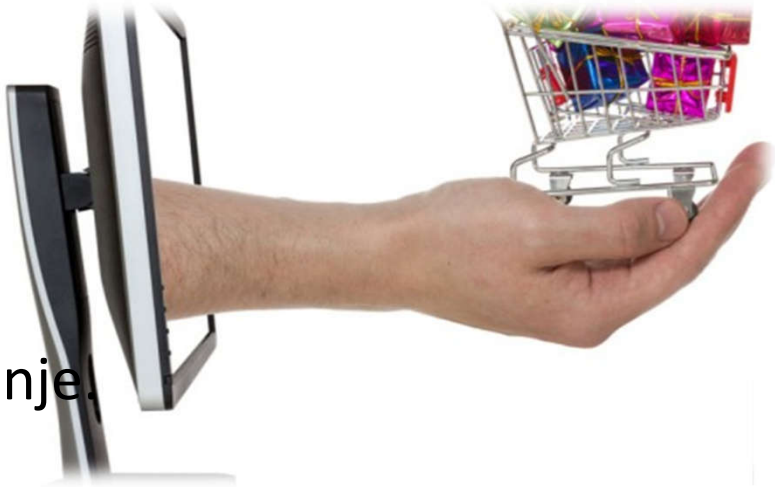


Platne kartice

- Ključnu ulogu u sistemu plaćanja ima **payment gateway** koji predstavlja ekvivalent terminalu na fizičkom mestu prodaje (POS).
- Payment gateway omogućava autorizaciju platnih kartica i siguran transfer informacija između mesta plaćanja preko Interneta (veb-sajt, mobilna aplikacija i sl.) i procesora plaćanja odgovarajuće banke.
- Payment gateway enkripcijom štiti osetljive informacije s kreditnih kartica.

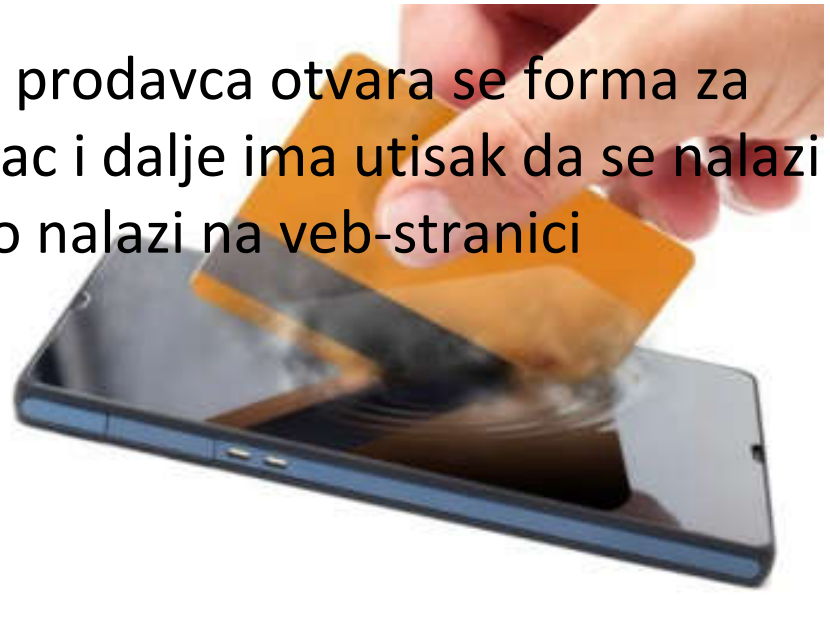
Platne kartice

- Proces plaćanja platnom karticom počinje tako što korisnik kartice (kupac) na Internet prodajnom mestu izabere artikal, zatim bira check out opciju.
- Nakon unosa ličnih podataka koji su potrebni za isporuku i plaćanje, kupac potvrđuje kupovinu.
- Nakon prijema narudžbine od kupca, prodavac šalje informaciju o početku plaćanja ka payment gateway.
- Kao odgovor kupac dobija šifru kupovine i adresu stranice za plaćanje.
- Kupac se tada preusmerava na odgovarajuću veb-stranicu za unos podataka o kartici, gde potvrđuje plaćanje.



Platne kartice

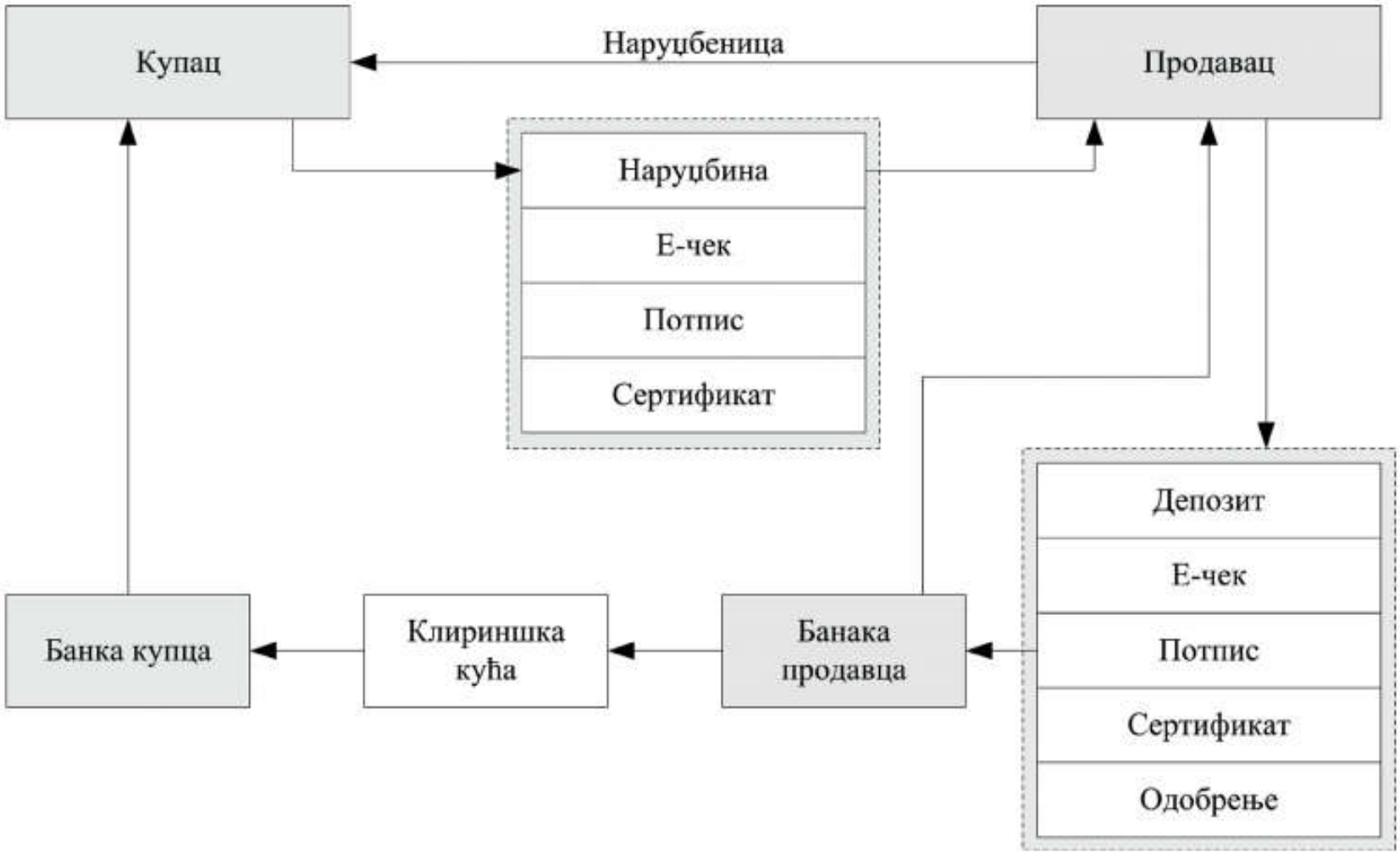
- Kod modela plaćanja platnim karticama postoje dva pristupa u preusmeravanju kupca s veb-sajta prodavca na sajt procesora plaćanja:
- **Preusmeravanje**. Kada korisnik izabere karticu kojom plaća, prebacuje se na veb-sajt procesora plaćanja. U adresi veb-brauzera menja se adresa, a korisnik se od tog trenutka nalazi na veb-sajtu procesora plaćanja.
- **Tunelovanje**. U okviru stranice sajta prodavca otvara se forma za unos podataka o platnoj kartici. Kupac i dalje ima utisak da se nalazi na veb-sajtu prodavca, ali se zapravo nalazi na veb-stranici procesora.



Elektronski ček

- Sistemi elektronskih čekova treba da prošire funkcionalnosti postojećih čekovnih računa, kako bi se omogućilo njihovo korišćenje za plaćanje u onlajn kupovini.
- Sistem elektronskog čeka zahteva da korisnik dobije od svoje banke elektronsku čekovnu knjižicu na odgovarajućem hardveru (CD, USB memorija, pametna kartica ili sl.).
- Elektronska čekovna knjižica sadrži digitalni potpis korisnika, kao i javni ključ banke izdavaoca.

Elektronski ček



Elektronski ček

- Tipičan primer plaćanja putem elektronskog čeka:

1. Kupac popunjava formu za porudžbinu i u prilogu postavlja nalog za plaćanje (e-ček), potpisuje ček privatnim ključem, dodaje sertifikat javnog ključa i ček šalje prodavcu.
2. Na strani prodavca dekriptuju se podaci primenom privatnog ključa, proverava se sertifikat kupca, potpis i ček, dodaje se depozit slip i zatvara depozit javnim sertifikatom. Ovi podaci se enkriptuju i šalju banci prodavca.
3. Banka prodavca proverava sve podatke na čeku i šalje ček na kliring.
4. Nakon kliringa na račun prodavca se dodaje odgovarajući iznos.
5. Kupac dobija potvrdnu informaciju o ishodu transakcije.

Elektronski novčanici

- Elektronski novčanici (E-wallet) su aplikacije koje predstavljaju nadgradnju standardnih instrumenata plaćanja, kao što su kartice ili transfer preko banke.
- Zasnivaju se na nalozima korisnika koji su otvoreni kod provajdera elektronskog novčanika.
- Nakon uplate depozita, korisnik može da kupuje na veb-sajtovima, tako što se uloguje na svoj elektronski novčanik.

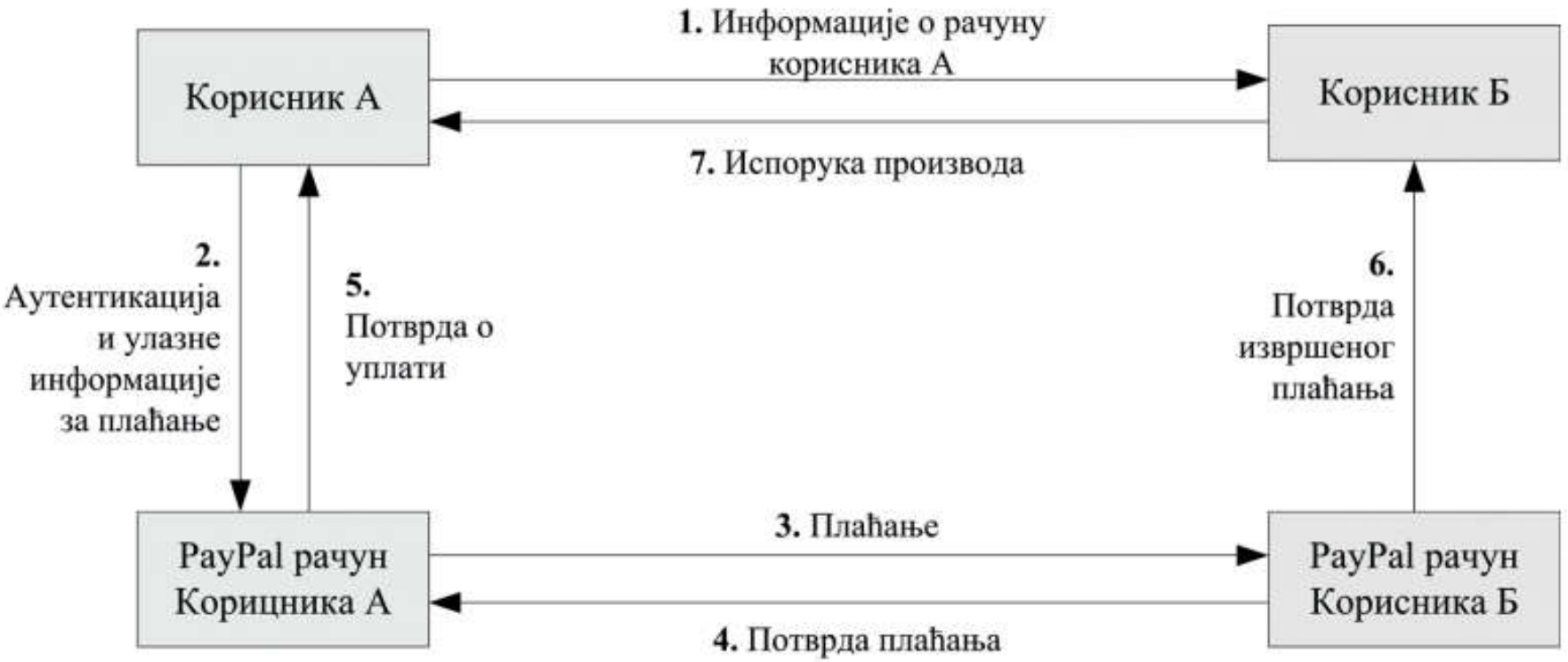
Elektronski novčanici

- Digitalni novčanik poseduje softversku i komponentu podataka. Softver obezbeđuje sigurnost i enkripciju vezanu za lične podatke i aktuelne transakcije.
- Komponenta podataka sadrži podatke kao što su adresa dostave, adresa računa, metode plaćanja (broj kreditne kartice, datum isteka, sigurnosni brojevi) i druge informacije.
- Najznačajniji provajderi elektronskog novčanika su Gugl i PayPal.

P2P plaćanja

- Peer-to-peer plaćanja, odnosno person-to-person plaćanja omogućavaju da kupac plati prodavcu, čak iako prodavac nema mogućnost da prihvati platne kartice.
- Najpoznatiji P2P sisteme plaćanja putem Interneta su PayPal, Square, Skrill (poznat pod prethodnim nazivom Moneybookers), Stripe i drugi.
- PayPal je sistem za plaćanje i transfer novca preko Interneta.
- Podrazumeva direktan prenos novca s jednog na drugi račun. Od 2003. godine je u vlasništvu E-bay-a.

Plaćanje putem PayPal-a



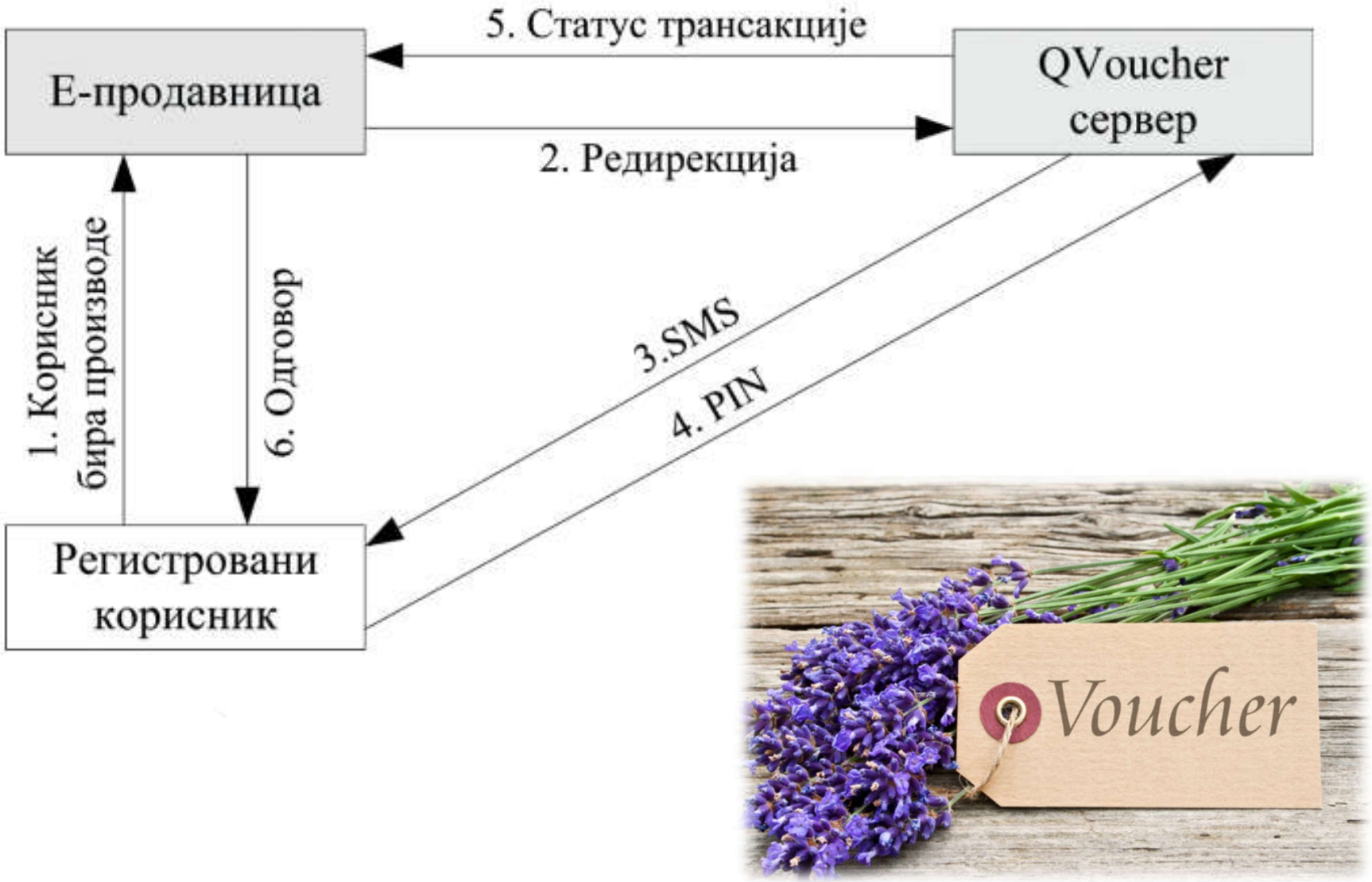
Plaćanje putem PayPal-a

- Prilikom otvaranja naloga, korisnik uplaćuje određena sredstva na svoj PayPal nalog.
- Kada kupac na nekom sajtu kupuje uslugu ili proizvod putem PayPala, novac se prebecuje direktno sa PayPal naloga kupca ka PayPal nalogu prodavca, bez ikakvog posredovanja banke u smislu procesiranja transakcija.
- U suštini, PayPal ima ulogu posrednika kome veruju obe strane i za to uzima određenu proviziju od prodavca za svaku transakciju.

Plaćanja vaučerima

- Plaćanje vaučerima spada u hibridna rešenja koja se često kreiraju u skladu s karakteristikama lokalnih tržišta.
- Jedno od najuspešnijih rešenja u našem okruženju je QVaucher.
- QVoucher je pripejd sistem plaćanja preko Interneta koji korisnicima omogućava da plaćaju proizvode i usluge bez kreditnih kartica i bankovnih računa.

Plaćanje putem Qvoucher-a

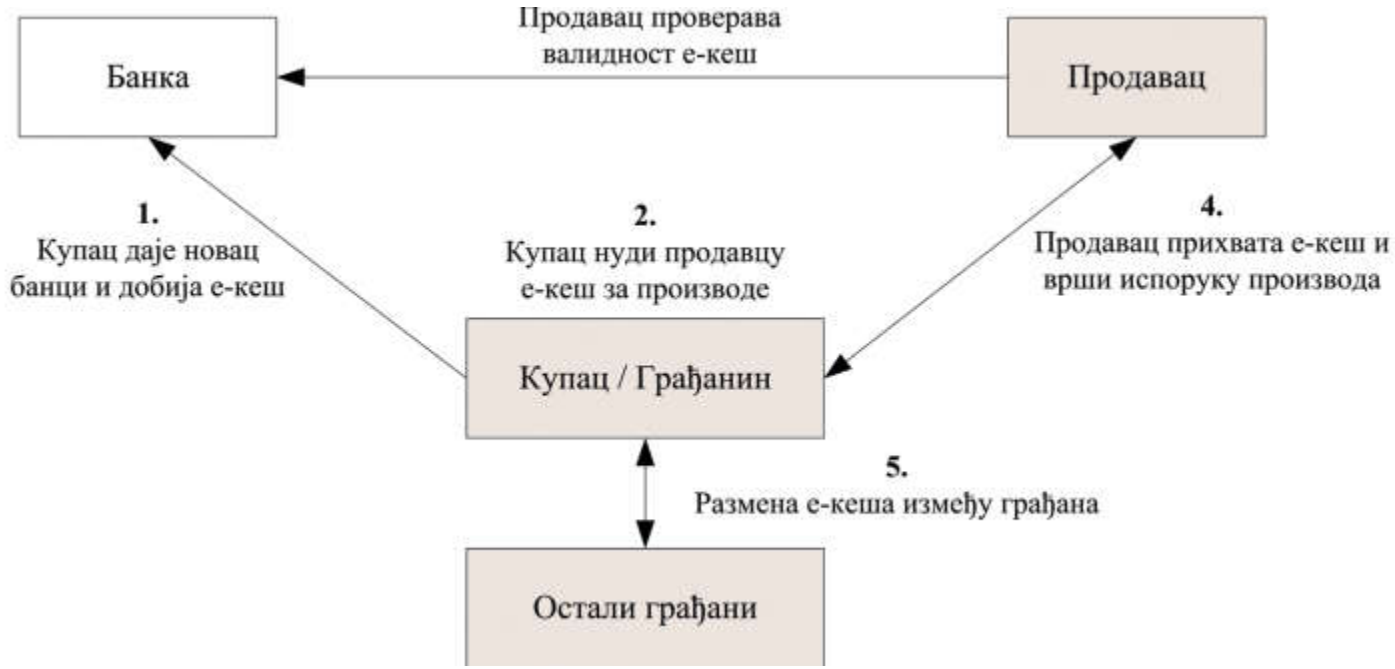


Plaćanje putem Qvoucher-a

- Podrazumeva se da je korisnik registrovan na sajtu QVoucher.rs i da ima uplaćena sredstva na QVoucher računu.
- Broj mobilnog telefona u okviru neke od mobilnih mreža u Republici Srbiji potreban je kao sredstvo za identifikaciju.
- Da bi korisnik potvrdio izvršenje transakcije potrebno je da ukuca PIN koji dobija putem SMS-a.
- Ovaj PIN se sastoji od šest cifara i različit je za svaku transakciju.
- Kada korisnik uspešno verifikuje transakciju, sredstva se prebacuju na račun prodavca, a korisnik se preusmerava na veb-sajt prodavca.

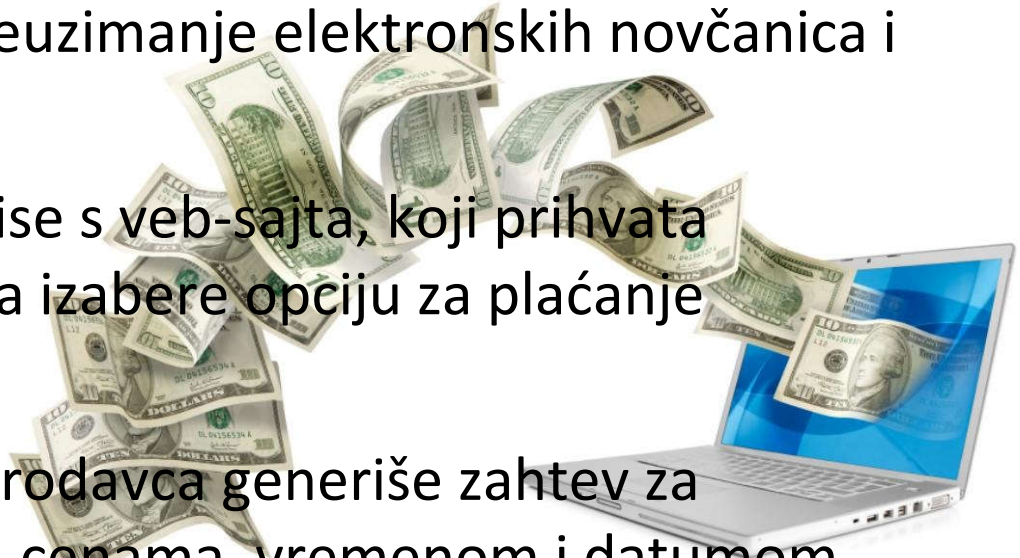
Elektronski novac

- Slično kao i tradicionalni keš, elektronski keš omogućava transakcije bez potrebe za korišćenjem usluga banke ili neke treće strane.
- E-keš se prebacuje direktno i odmah između prodavaca i kupca.
- E-keš se najčešće čuva na pametnim karticama, tako što se na čipu kartice skladišti novčana vrednost.



Elektronski novac

- Kupac od banke ili finansijske institucije dobija poseban softver za rad sa sistemom elektronskog keša.
- Digitalni novac se korišćenjem tog softvera može kupiti za običan novac. Softver omogućava preuzimanje elektronskih novčanica i smeštanje na računar kupca.
- Kada kupuje proizvode ili servise s veb-sajta, koji prihvata elektronski keš, kupac treba da izabere opciju za plaćanje elektronskim kešom.
- Softver instaliran na serveru prodavca generiše zahtev za plaćanjem, s listom proizvoda, cenama, vremenom i datumom.
- Kada kupac potvrdi zahtev, softver instaliran na računaru kupca šalje instrukciju za plaćanje. Elektronski keš se prebacuje na račun u banci prodavca.



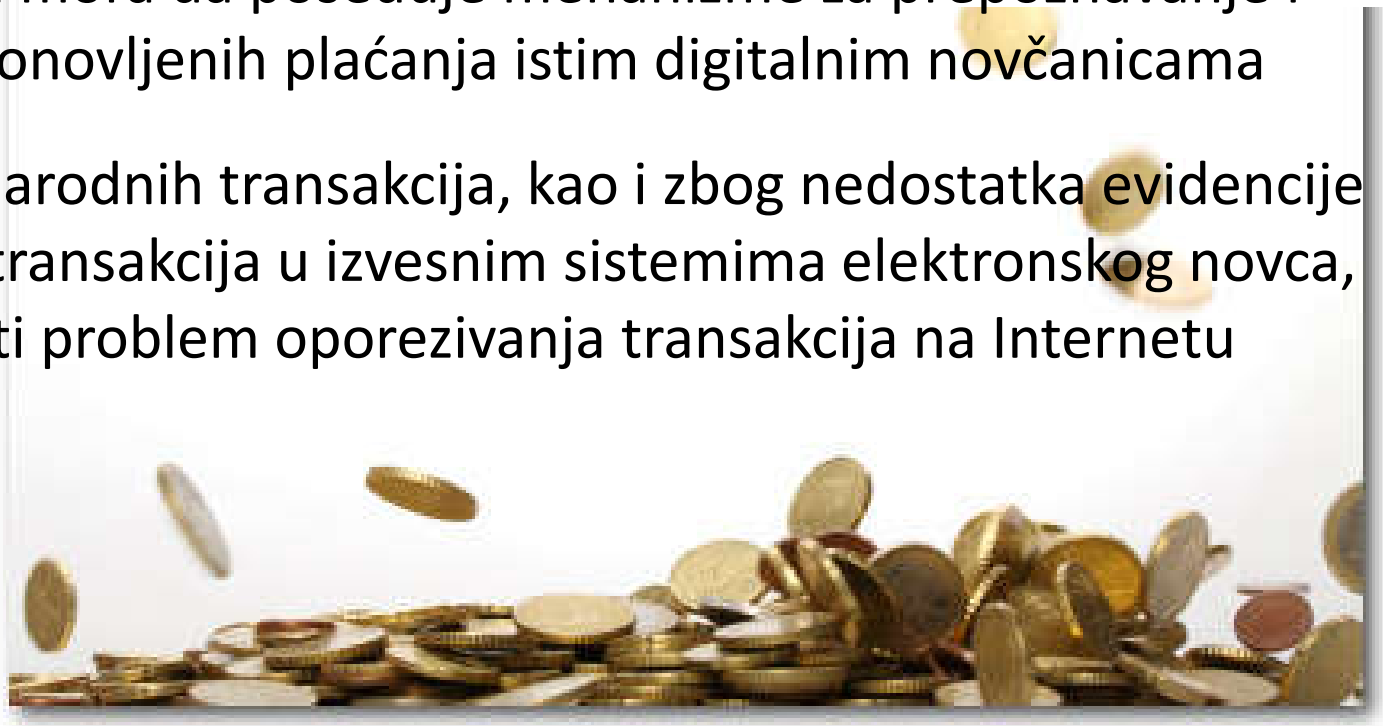
Elektronski novac

- Svaku elektronsku novčanicu emituje neka banka na ime deponovanog stvarnog novca, baš kao što je i svaka papirna novčanica emitovana na osnovu zlatne podloge
- Za razliku od platnih kartica, elektronski novac može da ostvari potpunu anonimnost kupca
- Ideja elektronskog novca je da se vrednost, umesto na papir, smešta u digitalnu memoriju kao niz cifara

Elektronski novac

- Sistem elektronskog novca trebalo bi da omogući i sitna plaćanja (tzv. **mikro plaćanja**)

- Platni sistem mora da poseduje mehanizme za prepoznavanje i prevenciju ponovljenih plaćanja istim digitalnim novčanicama
- Zbog međunarodnih transakcija, kao i zbog nedostatka evidencije za praćenje transakcija u izvesnim sistemima elektronskog novca, može se javiti problem oporezivanja transakcija na Internetu



Elektronski novac

- Sistemi zasnovani na digitalnim novčanicama imaju problem u vezi sa nominalnom vrednošću
  - Da bi se platio izvestan iznos moraju postojati digitalne novčanice sa odgovarajućom vrednošću, ili bi u suprotnom sistem morao biti sposoban da "vrati kusur" u obliku novih digitalnih novčanica
  - Alternativno rešenje – sve novčanice imaju istu nominalnu vrednost

Elektronski novac

- Pod uslovom da se navedeni problemi reše, može se uživati u brojnim prednostima elektronskog novca
  - Prenosiviji je i lakši za rukovanje od papirnog novca
  - Troškovi transfera novca preko Interneta znatno su manji od troškova transfera novca putem konvencionalnog bankarskog sistema
  - Kako elektronski novac koristi već postojeću mrežu i računare svojih korisnika, troškova transfera gotovo da i nema
  - Ako se novac izgubi, on se može odmah zameniti tako što se ponište nestale elektronske novčanice i zamene novim
  - Može ga koristiti svako ko ima pristup nekoj banci na Internetu

Ekonomske posledice elektronskog novca

- **Transnacionalnost** elektronskog novca ima potencijal da uzrokuje konflikt između virtuelnog tržišta i država, što dovodi u pitanje ulogu centralnih banaka kao arbitara nacionalne novčane mase

- Ako bi se neki elektronski novac proširio na susedne države, to bi moglo da dovede do ekonomskih sukoba između država

Ekonomske posledice elektronskog novca

- Ako se elektronski novac posmatra kao predstavnik realne valute, za njega mora da postoji određeni devizni kurs
  - U virtuelnom svetu će postojati devizno tržište na kome će svi moći da učestvuju
  - Masovno učešće na deviznim tržištima može da prouzrokuje nestabilnost deviznih kurseva
  - Devizni kursevi u virtuelnom i realnom svetu trebalo bi da budu jednaki
  - U realnom svetu razlika između prodajnog i kupovnog kursa iznosi 2% za prosečnog klijenta

Ekonomske posledice elektronskog novca

- Većina troškova biće eliminisana kod elektronskog novca
- Provizija za razmenu elektronskog novca treba da bude vrlo mala
- Korisnici elektronskog novca koristiće Internet da bi svoje modele potrošnje proširili u geografskom smislu
- Potrošači mogu na disku svog računara imati uskladišten veći broj valuta
- U slučaju da dođe do deprecijacije neke od tih valuta potrošači će, verovatno, nastojati da zamene tu vrstu elektronskog novca za neki vredniji i stabilniji oblik elektronskog novca
- Stvarna prisutnost digitalnog novca na tržištu je još uvek marginalna i može se zaključiti da i pored svih prednosti, elektronskom novcu predstoji težak put do šireg prihvatanja

Online i offline plaćanja elektronskim novcem

- Proces plaćanja elektronskim novcem može biti **online** i **offline**
- Kada je u pitanju online plaćanje, autentičnost digitalnih novčanica mora biti proverena odmah
- U slučaju online plaćanja neka digitalna novčanica se koristi samo jednom

Online i offline plaćanja elektronskim novcem

- Finansijska institucija mora da proveri autentičnost korišćenjem spiska svih novčanica koje su emitovane
- U slučaju offline plaćanja, digitalne novčanice se mogu koristiti više puta
- U cilju izbegavanja dvostrukog trošenja neophodno je smestiti informacije o korisniku ili korisnicima na samu novčanicu kako bi se provera mogla obaviti kasnije

Online i offline plaćanja elektronskim novcem

- Najpozantiji **online** sistemi su
  - E-Cash (DigiCash)
  - NetCash
  - BitCoin
- Najpoznatiji **offline** sistemi su
  - Mondex (MasterCard)
  - VisaCash (Visa)

- Iako postoje razlike, potencijalni koraci u transakcijama sa elektronskim novcem su sledeći

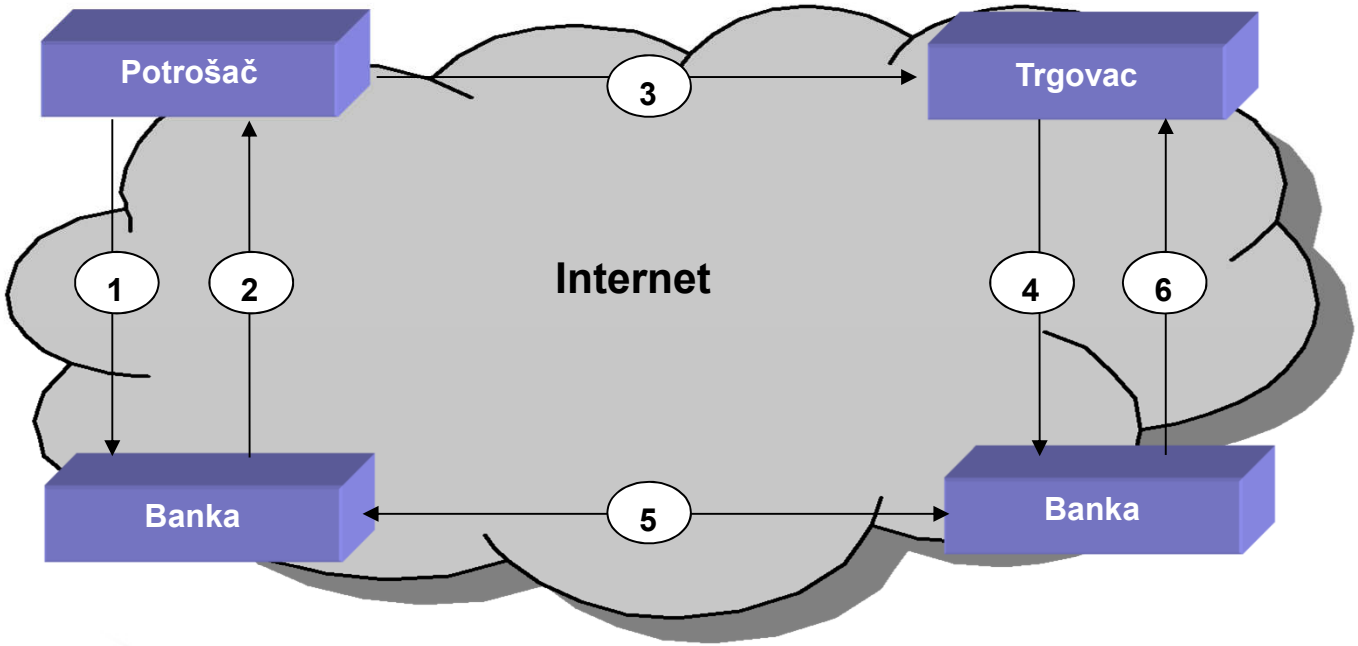
1. Potrošač otvara račun kod emitenta (npr. virtuelna banka) deponovanjem sredstava kod njega
2. Emitent čuva potrošačeva sredstva za buduća povlačenja, koja će vršiti oni koji od potrošača budu primili digitalnu novčanicu

Online i offline plaćanja elektronskim novcem

3. Kada potrošač poželi da kupuje preko Interneta, on pošalje šifrovanu poruku s digitalnim potpisom virtuelnoj banci zahtevajući finansiranje
4. Virtuelna banka zadužuje potrošačev račun i šalje mu digitalni novac na računar ili mobilni uređaj
   - Sistemi digitalnog novca mogu kreirati trag za reviziju transakcija ili mogu biti anonimni
   - U anonimnim sistemima virtuelna banka dodeljuje digitalne potpise koje samo ona može da kreira
   - Korisnici mogu dešifrovati takav potpis pomoću ključa koji im je dala virtuelna banka, kako bi se uverili da je ona emitovala novac
5. Potrošač prenosi digitalni novac prodavcu, koji može proveriti njegovu autentičnost i prebaciti ga na svoj račun kod virtuelne banke, poslati nekoj drugoj osobi ili prebaciti na drugi račun
6. Virtuelna banka će zaračunati potrošaču i/ili prodavcu proviziju za transakciju ili proviziju za usluge sistema

E-cash

- E-cash je anonimni digitalni novac čija se ispravnost proverava online, od strane odgovarajuće finansijske institucije
- E-cash sistem je razvila firma DigiCash 1995. godine



Proces plaćanja upotrebom E-casha

Online i offline plaćanja elektronskim novcem

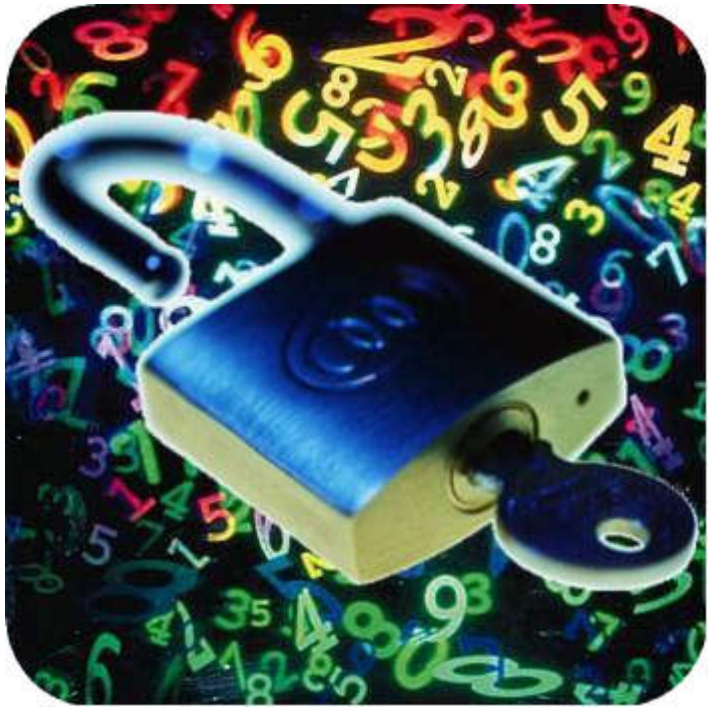
E-cash

- Proces plaćanja upotrebom E-casha obavlja se pomoću računara preko Interneta, na sledeći način:

1. Potrošač šalje novčanicu sa šifrovanim brojem svojoj finansijskoj instituciji (ovde sam potrošač generiše novčanice, ali ih ne može koristiti za trošenje dok ih njegova finansijska institucija ne overi)
2. Finansijska institucija mu vraća nazad overenu novčanicu, a da ne sazna njen serijski broj
3. Potrošač šalje trgovcu novčanicu sa otkrivenim serijskim brojem
4. Trgovac prosleđuje novčanicu svojoj finansijskoj instituciji
5. Kada potrošačeva finansijska institucija potvrdi da je dotična novčanica overena i da nije već potrošena, finansijske institucije vrše “kliring” (završetak transakcije)
6. Trgovac dobija potvrdu, a saldo na njegom računu se povećava za dati iznos, na račun sredstava povučenih od potrošača u trenutku izdavanja digitalnih novčanica

E-cash

- Bezbednost E-casha postiže se upotrebom asimetričnog kriptografskog algoritma
- Pristup računu može biti dodatno zaštićen upotrebom ličnih lozinki
- Problem je što su troškovi provere autentičnosti digitalnih novčanica relatvno veliki, jer provera treba da se obavi online
- Znači da je pogodnost ovog sistema za mikro-plaćanja pod znakom pitanja
- E-cash nije ostvario globalno širenje na Internetu, delimično zbog naplaćivanja taksi samo emitentima a ne i korisnicima, a uglavnom zbog odlučnog insistiranja na potpunoj anonimnosti, čime je ukinuta bilo kakva mogućnost praćenja transakcija

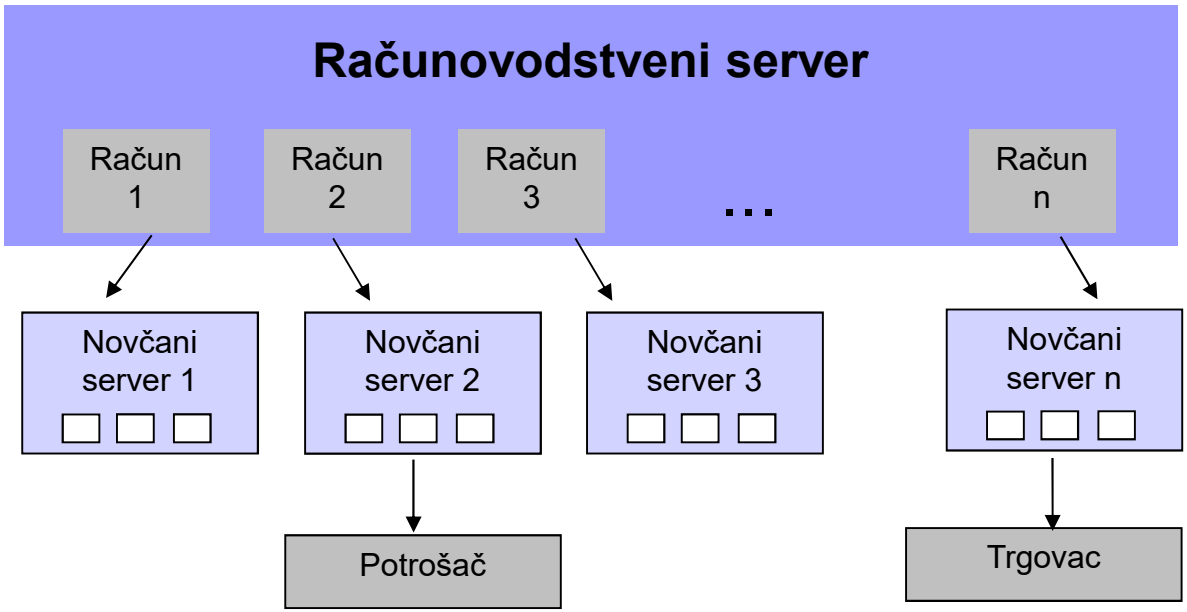


NetCash

- NetCash metoda je razvijena na Univerzitetu Južne Kalifornije u SAD
- Značajna karakteristika ovog projekta jeste upotreba postojećih računovodstvenih sistema i procedura u finansijskim institucijama, što će uticati na smanjivanje početnih investicija
- Nasuprot E-Cashu ova metoda zasnovana je na decentralizovanom pristupu
- Problemi u vezi s velikim brojem novčanica i učesnika mogu se rešiti mnogo lakše
- Prihvaćena je delimična anonimnost, a potrebna je i kooperacija svih finansijskih institucija koje učestvuju u sistemu
- Sistem se zasniva na distribuiranim novčanim serverima
- Novčani serveri predstavljaju lokacije na kojima se anonimni novac zamenjuje sa neanonimnim

NetCash

- Svaki novčani server (koji obavlja kliring) poseduje jedan račun na računovodstvenom serveru
- Neophodno je da se potvrdi integritet ovih servera i da novčani serveri mogu da primaju novčanice sa drugih novčanih servera
- NetCash novčanice imaju nominalnu vrednost i serijski broj



Sistem novčanih sredstava servera kod NetCasha

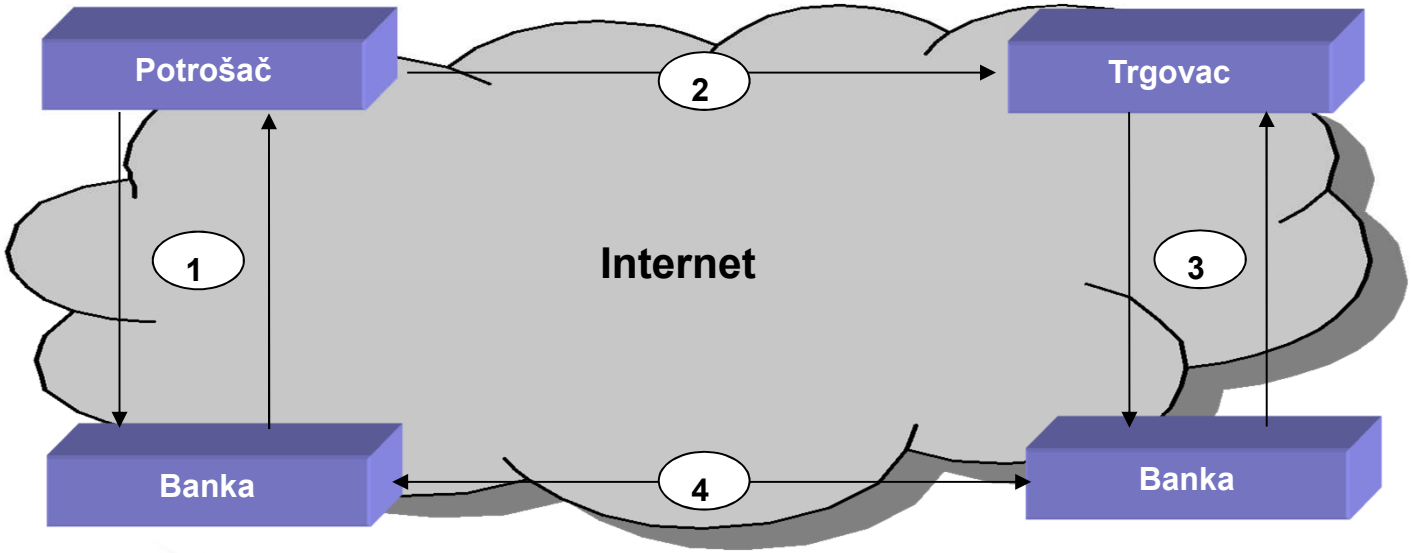
NetCash

- Proces plaćanja upotrebom NetCasha obavlja se pomoću računara i preko Interneta na sledeći način:
  1. Potrošač podiže digitalne novčanice u svojoj finansijskoj instituciji preko novčanog servera (serijski brojevi ovih novčanica su vidljivi i poznati emisinom serveru)
  2. Potrošač šalje digitalne novčanice trgovcu, šifrovane pomoću asimetričnog algoritma, javnim ključem emisionog servera
     - Ovako šifrovanu novčanicu može da dešifruje samo emisioni server
  3. Trgovac podnosi ove novčanice svojoj finansijskoj instistuciji, koja ih prosleđuje emisionom serveru na proveru
     - On zatim od svog novčanog servera dobija nove neanonimne novčanice, ili se dati iznos prebacuje na njegov račun
  4. Finansijske institucije obavljaju kliring

NETCASH
SMART MONEY MANAGEMENT

NetCash

- Bezbednost se postiže pomoću kriptografskih algoritama
- Kao i slučaju E-casha, i ova metoda zahteva dosta online komuniciranja
- Svaka osoba može da prima NetCash novčanice, jer sistem omogućava slobodnu razmenu novčanica



Proces plaćanja upotrebom NetCasha

BitCoin

- BitCoin je P2P sistem elektronskog plaćanja uveden 2009. godine koji sve više dobija na popularnosti
- Softver na kom je zasnovan je open-source
- Zovu ga “decentralizovana valuta” jer nije vezan ni za jednu određenu banku ili finansijsku instituciju

- Distribuirani serveri sadrže registre (*ledger*) u kojima se čuvaju detalji o stanjima na računima i transakcijama

BitCoin

- Mreži servera, kao i korisnika, može da se priključi svako
- Korisnici koriste valutu pomoću digitalnog “novčanika” – softvera za personalne računare i druge uređaje
- Korisnici do valute mogu doći na dva načina:
  - Zamenom za klasičnu valutu
  - “Rudarenjem” (*mining*), odnosno “društveno korisnim radom” u održavanju registara

- Bezbednost se postiže asimetričnim kriptografskim algoritmima
- Anonimnost nije zagarantovana
- BitCoin-e je moguće ukrasti, na način da je refundacija štete nemoguća

Mikro plaćanja

- Mikro plaćanja su elektronska plaćanja male vrednosti (u rasponu od nekoliko dolara do nekoliko centi, pa i manje), koja su specijalno dizajnirana za elektronsku trgovinu na Internetu, pre svega za trgovinu nematerijalnim dobrima
- Najpozantiji sistemi su:
  1. **MilliCent**
     - Projekat koji je razvijen u istraživačko-razvojnom odeljenju DEC korporacije (Digital Equipment Corporation)
     - Dizajniran je tako da podržava kupovine u iznosima od jednog centa, pa čak i manjim
     - Da bi se postigao ovaj cilj, u MilliCent sistemu žrtvovane su neke pogodnosti koje pružaju drugi modeli: on ne nudi anonimnost plaćanja

Mikro plaćanja

2. NetBill

- Istraživački projekat koji je započet na Institutu za informacione tehnologije pri Carnegie Mellon univerzitetu, u saradnji sa organizacijama Mellon Bankom i Visom
- U ovom sistemu NetBill ima ulogu treće strane, koja vrši proveru autentičnosti, upravlja računima, vrši obradu transakcija, fakturisanje i informisanje klijenata i korisnika u mreži

3. CyberCash

- Predstavili su svoju verziju sistema digitalnog novca za mikro plaćanja oktobra 1996. godine, pod nazivom CyberCoin
- U suštini, ovaj sistem se zasniva na računovodstvenom transferu odgovarajućih iznosa
- CyberCash vrši transfer novca sa potrošačevog privremenog računa na trgovčev privremeni račun koji su, posebno za tu namenu, kreirani u CyberCash banci u Virdžiniji

Elektronski prenos novčanih sredstava

- Početkom 1970-ih, banke su počele da istražuju rešenja za pristup novčanim sredstvima preko elektronskih terminala
- Mnoge finansijske institucije nude oba pristupa – takozvani elektronski prenos novčanih sredstava (**EFT – *Electronic Fund Transfer***), i klasičan prenos novčanih sredstava baziran na papirnim dokumentima
- EFT se može ostvariti korišćenjem sopstvene računarske mreže banaka
- Svaki kupac u tom slučaju može da pristupi svojim novčanim sredstvima preko elektronskog terminala u okviru mreže banaka
- Postoji sve više i više finansijskih institucija koje integrišu sopstvene mreže u jednu veliku mrežu koja služi korisnicima mnogih banaka i finansijskih institucija

Elektronski prenos novčanih sredstava

- Postoji mnogo problema u vezi sa zaštitom, koje treba rešiti pre nego što se EFT mreža instalira, na primer kako korisnici mogu da se identifikuju pre transakcija, kako može da se osigura autentičnost i integritet transakcija, itd.
- Prihvaćeno je mišljenje da je dobar način za identifikaciju korisnika korišćenje tajnog ličnog identifikacionog broja (**PIN – *Personal Identification Number***) zajedno sa bankarskom karticom koja nosi ostale informacije potrebne za pokretanje transakcija

Elektronski prenos novčanih sredstava

- Zaštita PIN-a, a samim tim i bankarske kartice, presudna je za celokupnu bezbednost EFT-a transakcija
- Bankarske kartice se mogu izgubiti, ukrasti ili zaboraviti
  - U takvim slučajevima, jedina postojeća kontramera protiv neautorizovanog pristupa je tajni PIN
  - Ovo je razlog zašto PIN treba da zna samo legitimni vlasnik kartice, i on nikad ne treba da se čuva ili prenosi u otvorenom obliku

Elektronski prenos novčanih sredstava

- Dužina PIN-ova treba da bude dovoljno velika tako da je mogućnost pogađanja tačne vrednosti u slučaju grubog napada prihvatljivo mala
- PIN-ovi treba da budu kratki da bi vlasnici mogli da ih zapamte (preporučena dužina je od četiri do osam cifara)
- PIN-ove mogu izabrati bilo banka ili vlasnici kartica

Elektronski prenos novčanih sredstava

- Ako banka odabira PIN, ona usvaja jednu od dve procedure:

1. PIN-ovi se generišu kriptografski od brojeva računa vlasnika kartice
   - Prednost ove procedure je što zapis PIN-a ne mora da se čuva unutar EFT sistema
   - Mana je što promena PIN-a zahteva odabiranje ili novog računa korisnika, ili novi kriptografski ključ
   - Kako se svi PIN-ovi izračunavaju korišćenjem istog ključa, promena jednog zahteva promenu svih PIN-ova
2. Banka odabira PIN slučajno i istovremeno

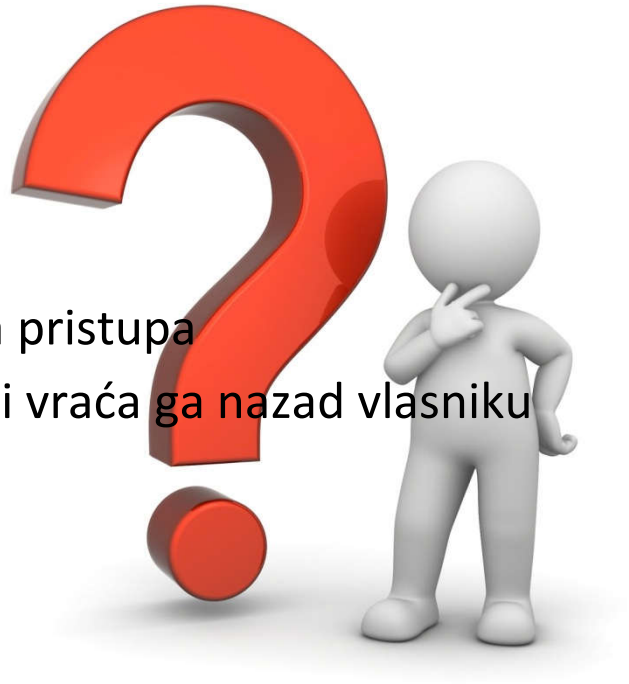
čuva zapis u obliku prikladnog kriptograma

(tačan oblik PIN-a ne treba nikad da se prikaže

unutar EFT sistema)

Elektronski prenos novčanih sredstava

- Vlasnici kartica takođe mogu da biraju PIN-ove
  - Najbolja procedura za vlasnike kartica je odabiranje PIN-a slučajnim izborom
  - Jednom kada se odaber PIN, banka treba da se obavesti o tome
  - PIN-ovi mogu da se pošalju u banku preporučenom pošiljkom, ili da se unesu preko bezbednih terminala, koji kriptuju PIN, i uskladište ga u arhivu banke
- Ljudi vrlo često zaborave PIN
  - Banke treba unapred da pripreme specijalne procedure koje će rešiti ovakve slučajeve
  - Procedure mogu da usvoje jedan ili dva različita pristupa
    - Prvi radi na otkrivanju zaboravljenog PIN-a, i vraća ga nazad vlasniku
    - Drugi generiše novi PIN



Elektronski prenos novčanih sredstava

- Realizacija EFT sistema sa PIN-om i tajnim ključem
  - Da bismo povećali zaštitu EFT sistema, naročito za vreme inicijalizacije, možemo produžiti PIN-ove i/ili uvesti kartice čije je dupliciranje teško i skupo
  - Istraživanja su pokazala da ako je dužina PIN-a veća od osam decimalnih cifara, broj pogrešnih pokušaja inicijalizacije se povećava usled činjenice da je tako dugačak PIN teško zapamtiti
  - Distribucija bankarskih kartica otpornih na falsifikovanje je jedino krajnje rešenje
  - Prvo rešenje - svaka kartica sadrži dve utisnute poruke: broj računa (***Primary Account Number* – PAN**) i lični ključ (***Personal Key* – PK**)
    - PK izabira distributer na slučajan način i njegova dužina zavisi od korišćenog algoritma šifrovanja
  - Drugo rešenje - bankarska kartica sadrži PAN, PK, i kod za ličnu autentifikaciju (PAC)

Elektronski prenos novčanih sredstava

- Zahtevi u pogledu PIN brojeva
  - Postoji nekoliko zahteva za bezbednost, koji se odnose na identifikaciju korisnika baziranih na PIN-ovima i bankarskim karticama, i to su sledeći:
    - PIN mora da se čuva u tajnosti sve vreme
    - PIN ne sme biti zapisan na kartici
    - Kartica treba da sadrži jedinstven broj (PAN) koji odgovara PIN-u vlasnika kartice
    - Ako kartica sadrži kod za ličnu autentifikaciju (PAC), on mora da zavisi od PIN-a ali otkrivanje PIN-a iz osnove PAC-a mora da bude nepraktično
    - Proces identifikacije mora biti vremenski zavisan (da spreči ponovni napad)

Elektronski prenos novčanih sredstava

- Zahtevi u pogledu PIN brojeva
  - Skup zahteva za bezbednost koji se odnose na kod za autentifikaciju poruke (MAC) je sledeći:
    - MAC mora da sadrži opis transakcije (poruka zahteva za transakcijom), PIN vlasnika kartice, i tekući datum i vreme
    - Izračunavanje PIN-a mora da bude veoma teško iz osnove MAC-a
    - Vremenska referenca MAC-a mora da se determiniše nazavisno od distributera
    - Poruka (poruke) obuhvaćena za vreme faze identifikacije vlasnika kartice mora biti udružena sa porukom (porukama) generisanom u drugoj fazi komunikacionog postupka
  - Sledeći korak za povećanje bezbednosti EFT sistema je učinjen uvođenjem smart kartica
  - Primena ovih kartica je praktično uklonila nezaštićen protok informacija između čitača kartice i bezbednosnog modula u fazi identifikacije

Inteligentne kartice

- Preteča inteligentnih su klasične:
  - kreditne i debitne kartice
- Uprkos svim poboljšanjima koje su donele,

  klasične kartice su se pokazale kao nepogodne za elektronski prenos sredstava, odnosno online trgovinu
- Internet je mreža kojom ne bi trebalo da putuju nezaštićeni ili slabo zaštićeni osetljivi podaci, kao što su brojevi kreditnih, odnosno debitnih kartica, i odgovarajući kodovi za njihovo aktiviranje
- Po mogućstvu bi trebalo izbeći i da se brojevi kartica skladište na serverima njihovih primalaca, jer su krajnje tačke Internet komunikacije često primamljiva meta neovlašćenih pristupa
- Mnogo je otkrivenih zloupotreba platnih kartica do kojih je iz navedenih razloga došlo, a sasvim je izvesno da ih je još više ostalo neotkriveno

Smart platne kartice

- Smart kartica je plastična kartica, koja po izgledu podseća na običnu kreditnu ili debitnu karticu s tim da poseduje jedan detalj koji je odvaja od njih, a to je integrisano kolo, odnosno čip, na kome se nalaze procesor i memorija
- Tradicionalna kreditna ili debitna kartica čuva podatke na magnetnoj traci
  - Traka je sačinjena od tri staze na kojima se čuvaju podaci
  - Nijedna od ovih staza nema kapacitet za čuvanje velike količine podataka
  - Upisani podaci podložni su spoljnim uticajima, te mogu biti promenjeni, izbrisani ili oštećeni, slučajno ili namerno
  - Iako je ostavljena mogućnost i za čitanje i za upisivanje podataka, zbog nedovoljne bezbednosti i praktičnih razloga upisivanje se gotovo ne koristi, tako da ovu karticu možemo nazvati samo memorijskom, odnosno karticom na kojoj se podaci samo čuvaju

Smart platne kartice

- Smart kartica ima oko 100 puta više memorijskog prostora i procesor koji omogućava izvršavanje raznih algoritama
  - Ceo proces (npr. kriptovanje) počinje, traje i završava se na samoj kartici i nikakvi podaci ne napuštaju karticu što sistem čini izolovanim od spoljnjeg sveta
  - Samo vlasnik kartice može je aktivirati
  - unošenjem odgovarajućeg ličnog identifikacionog broja (PIN)

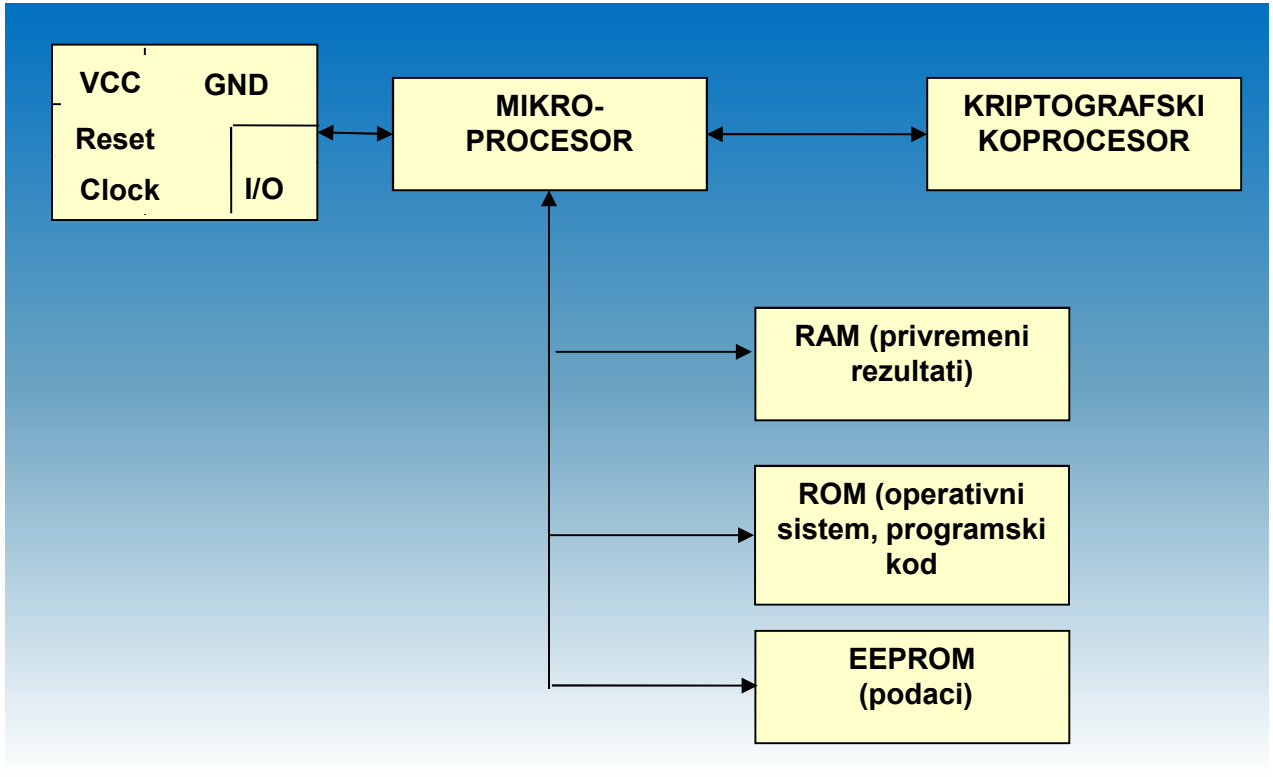
Smart platne kartice

- Najveća snaga *Smart Card* tehnologije upravo je u raznovrsnosti mogućih primena
  - Moguće je razviti raznovrsne aplikacije u oblastima kao što su: informacione tehnologije, telefonija, bankarstvo, zdravstvo, itd.
- Trenutno su u opticaju stotine miliona smart kartica u raznim oblastima sa tendencijom daljeg razvoja
- Nema nikakve sumnje da je prelazak sa magnetne trake na čip neminovan sled događaja

Razvoj smart tehnologije

- Smart kartica predstavlja personalni računar u malom
  - Uključuje:
    - procesor (CPU) pomoću koga se vrše razna izračunavanja
    - Read-Only Memory (ROM) – memoriju na kojoj se nalazi operativni sistem
    - Random Access Memory (RAM) – memoriju koja se koristi za privremeno skladištenje prilikom rada procesora
    - Electronically Erasable and Programmable Read Only Memory (EEPROM) – memoriju u kojoj su smešteni podaci od interesa
  - Stariji modeli smart kartica tipično poseduju 8-bitni procesor koji radi na frekvenciji od oko 5Mhz, dok su u poslednjih nekoliko godina sve zastupljeniji 32-bitni RISC procesori, koji rade na 25-32 Mhz
  - Operativni sistem je odgovoran za bezbednost podataka, i on vodi računa o pravima pristupa pojedinim fajlovima

Razvoj smart tehnologije



Unutrašnja struktura smart kartice

Razvoj smart tehnologije

- Smart kartica ne poseduje tastaturu niti bilo kakav displej
- Ona može da funkcioniše tek u kombinaciji sa odgovarajućim uređajem za čitanje smart kartica – **CAD (*Card Acceptance Device*)**
- Dva su osnovna tipa smart kartica – kontaktne i beskontaktne
  - Kontaktne smart kartice poseduju električne kontakte pomoću kojih dolaze u dodir sa električnim kontaktima čitača, i njih je potrebno uvući u čitač
  - Beskontaktne kartice imaju u sebi navojak žice koji se ponaša kao antena, i preko njega komuniciraju sa okolinom, što je naročito korisno za transakcije koje se moraju obaviti velikom brzinom

- Smart kartice mogu se razlikovati i po dimenzijama, i pored kartica standardnih dimenzija (veličine klasične platne kartice) postoje i SIM-kartice, koje su manjih dimenzija, prilagođene upotrebi u mobilnoj telefoniji

Razvoj smart tehnologije

Faza proizvodnje

- izvode je proizvođači čipa, i tokom te faze se u čip utiskuje tzv. ključ proizvođača, jedinstven za svaku smart karticu, ali izveden na osnovu glavnog ključa proizvođača

Faza pre-personalizacije

- čip se postavlja na karticu i testira, a ključ proizvođača se zamenjuje tzv. ličnim ključem, i nadalje se zabranjuje fizički pristup memoriji, a dopušta se isključivo logički

Faza personalizacije

- upisuju se podaci o korisniku, upisuju se PIN, deblokirajući PIN, aplikacije i ostali podaci od interesa, a faza se završava postavljanjem ključa koji ukazuje na to da je kartica nadalje u fazi korišćenja

Faza korišćenja

- korisnik redovno koristi karticu, a prava pristupa pojedinim podacima reguliše aktivna aplikacija koja je pod kontrolom operativnog sistema

Faza blokiranja

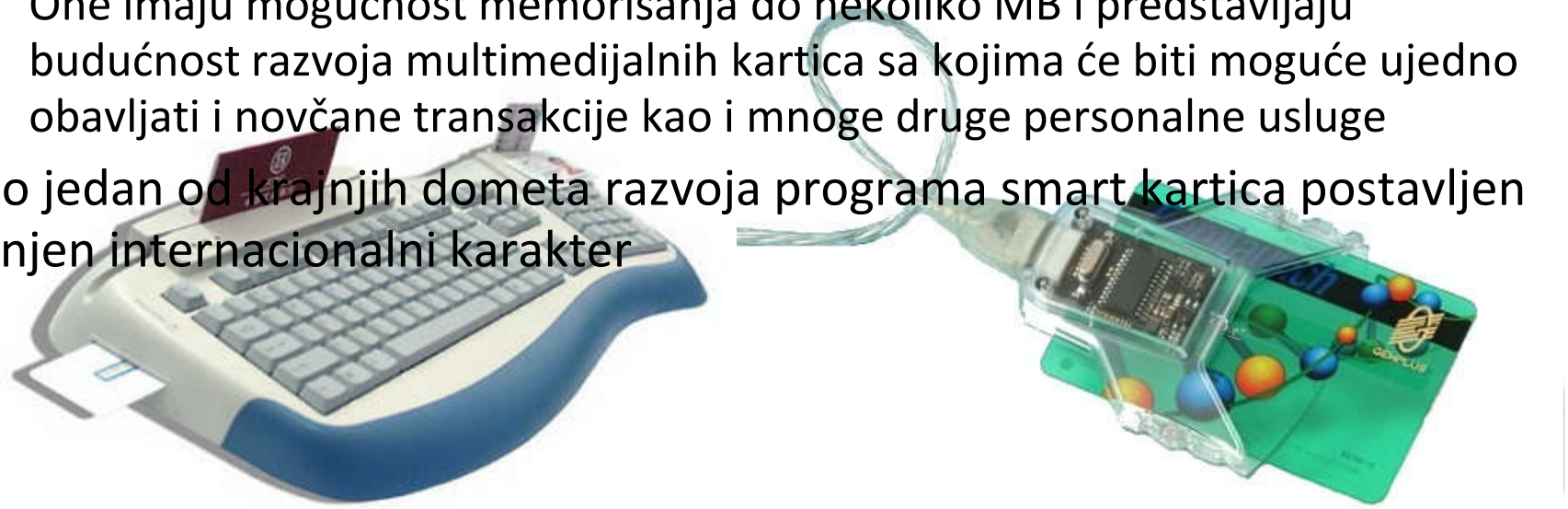
- kartica se poništava kada prestane potreba za njenim korišćenjem, jer se iz tehničkih, ali i bezbednosnih razloga ne preporučuje da pređe u ruke drugog vlasnika

Razvoj smart tehnologije

- Stvaranje multifunkcionalne jeftine smart kartice koja će istovremeno biti i platna i identifikaciona kartica i omogućavati pristup mobilnoj mreži, predstavlja ozbiljan zadatak, ali je to neophodno ukoliko se želi da ona bude široko prihvaćena
  - Postoji više načina da se to postigne:
    - Kreiranjem zajedničkih standarda za operativni sistem
    - Stvaranjem zajedničkog interfejsa između aplikacija i operativnog sistema
    - Usvajanjem jednog operativnog sistema koji se nalazi u najširoj primeni
- Kao prilog standardizaciji operativnog sistema za kartice, trebalo bi usaglasiti standarde za programske aplikacije koje koriste smart kartice kao deo sistema

Razvoj smart tehnologije

- Aplikacije komuniciraju sa čitačima smart kartica koji čitaju ili upisuju podatke sa smart kartice
- Čitači mogu biti povezani sa personalnim računarima, integrisani u ATM uređaje (bankomate), ugrađeni u POS (*Point of Sale*) terminale, mobilne telefone, ili samostalni sa sopstvenim malim LCD ekranom i numeričkom tastaturom
- Laserske kartice su nastavak razvoja smart tehnologije u pravcu povećanja hardverskih resursa
  - One imaju mogućnost memorisanja do nekoliko MB i predstavljaju budućnost razvoja multimedijalnih kartica sa kojima će biti moguće ujedno obavljati i novčane transakcije kao i mnoge druge personalne usluge
- Kao jedan od krajnjih dometa razvoja programa smart kartica postavljen je njen internacionalni karakter



Bezbednost smart kartica

- Smart kartica se radi sprečavanja zloupotrebe i kopiranja oslanja na kontrolu pristupa podacima koji se nalaze na EEPROM-u pomoću sopstvenog bezbednosnog operativnog sistema smeštenog na ROM-u
- U EEPROM-u se mogu nalaziti 1024-bitni RSA ključ, lični podaci o vlasniku kartice, broj tekućeg računa, sertifikati, te je od velikog interesa da ovi podaci ne budu izloženi zloupotrebi
- Može se osigurati da deo podataka bude vidljiv od strane čitača smart kartice a da deo ne bude i da nikako ne može napustiti karticu
- Dobro dizajnirani sistemi koriste višestruke mere bezbednosti
- Da bi se kartica koristila, neophodno je znati odgovarajući kod za aktiviranje
- – PIN (*Personal Identification Number*)
- Postojanje PIN-a eliminiše mogućnost zloupotrebe kartice u slučaju krađe ili gubitka

Bezbednost smart kartica

- Identifikacija pomoću PIN-a višestruko je bezbednija od bilo kog drugog načina identifikovanja iz sledećih razloga:
  - PIN nikada ne putuje mrežom i otporan je na napade tipa bruteforce ili dictionary
  - Polise koje regulišu dužinu i učestanost promene PIN-a mogu biti manje restriktivne od onih za lozinku – na taj način se izbegava ugrožavanje bezbednosti sistema od strane osoblja zapisivanjem identifikacionih kodova na papire ili u datoteke
- Razvoj smart tehnologije ide u pravcu generisanja i drugih tehnika
  - Tako je na planu bezbednosti usvojen metod generisanja otiska prsta korisnika na čipu kartice, kako bi se prilikom isplate u banci ili maloprodajnoj mreži preko čitača obezbedila provera identiteta na licu mesta
  - Razvojem uređaja za proizvodnju kartica sa ultra-grafikom usvojena je i tehnologija generisanja elektronske fotografije korisnika na plastičnoj podlozi same kartice preko tzv. ***smart printera***

Bezbednost smart kartica

- Smart kartica može da potvrdi svoj identitet zahvaljujući svom privatnom ključu
- Čitač kartice može proveriti autentičnost smart kartice šaljući joj slučajno odabranu digitalnu reč
- Od kartice se tada zahteva da potpiše poslatu reč svojim privatnim ključem, koji samo ona poseduje, i vrati tako potpisanu reč čitaču, koji uz pomoć javnog ključa kartice vrši verifikaciju
- Podaci koji se nalaze na kartici nikada ne napuštaju bezbedno okruženje, otporni su na sve napade na operativni sistem
- Logički napad na smart karticu podrazumeva dovođenje nepredviđenog napona u cilju ometanja funkcije EEPROM-a na kom su smešteni podaci od interesa
- Kod nekih procesora dovođenje nepredviđenih napona može da dovede do brisanja sigurnosnog bita bez oštećenja podataka, dok kod drugih procesora može da ugrozi generisanje ključa

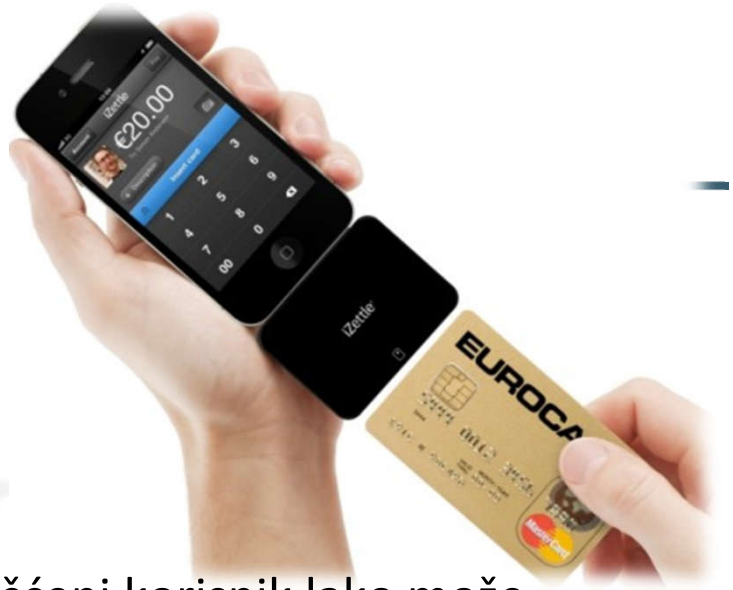
Bezbednost smart kartica

- Iz bezbednosnih razloga, moguća je i ugradnja senzora koji reaguje na nepredviđene uslove, ali se to rešenje izbegava, jer se ovakvi senzori veoma često oglašavaju i kad ne treba
- Fizički napad na smart karticu podrazumeva da se čip prethodno ukloni iz kartice bez oštećenja, a zatim se pristupi nekoj od tehnika napada na sam čip
  - Moguć je reverzni inženjering čipa, čime se otkrivaju struktura i funkcionisanje čipa, te je samim tim lakše doći do podataka sakrivenih u EEPROM-u
  - Mogući pravac napada je i brisanje sigurnosnog bita fokusiranim UV svetlom, kao i analiza čitave površine čipa naročito osetljivim mikroskopom
- Ovo su tehnike koje su veoma skupe, i samim tim ograničene na dobro finansirane laboratorije, a pojedincima nedostupne

Primene smart kartica

- **Finansije**
  - Smart kartica može poslužiti kao univerzalna platna kartica, slično klasičnoj platnoj kartici, ali u daleko bezbednijem okruženju
  - Smart tehnologija pruža mogućnost dizajniranja sertifikovanih bankarskih kartica koje je moguće puniti novčanim depozitom (elektronski keš) na bazi koncepta koji je poznat kao elektronski novčanik (*electronic purse*)
- **Identifikacija**
  - Smart kartica može poslužiti kao vozačka dozvola, studentska iskaznica, ili jednostavno kao univerzalna legitimacija
  - Može poslužiti i za autorizaciju, odnosno, kontrolu pristupa objektima

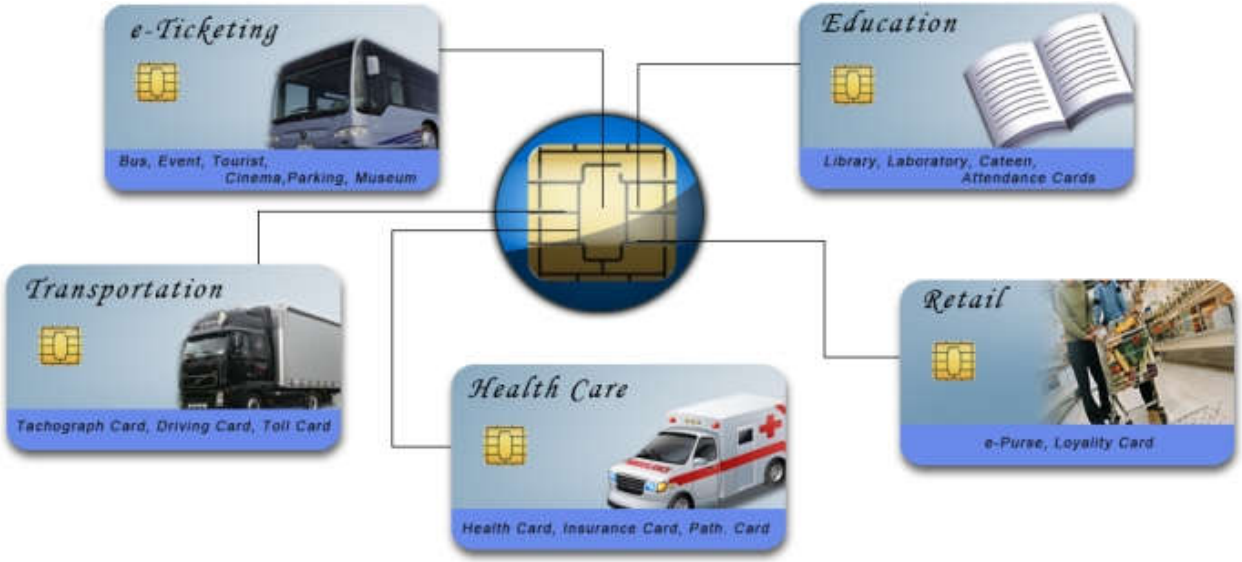
Primene smart kartica



- **Telefonija**
  - Za razliku od obične SIM kartice koju neovlašćeni korisnik lako može zloupotrebiti ako dozna PIN njenog vlasnika, smart kartica obezbeđuje pouzdanu identifikaciju korisnika u GSM sistemu, a samim tim i bezbedno iniciranje poziva
  - Postoje servisi koji omogućavaju online transakcije mobilnim telefonom, pri kojima se iznos automatski skida sa prepaid kartice
  - Skremblovanje poverljivih telefonskih razgovora, čime se onemogućava njihovo prisluškivanje od strane treće osobe
- **Informacione tehnologije**
  - Najčešća primena je kontrola pristupa računarima i računarskim mrežama
  - Prvi modem sa integrisanim čitačem smart kartica predstavljen je još 1996. godine
  - Svi značajni proizvođači računara već su proizveli hardver koji podržava funkcionalnost smart kartice

Inteligentne kartice

Primene smart kartica



- **Saobraćaj**
  - Primene u ovoj oblasti su brojne, počev od elektronskih karata i vaučera, koji u mnogome mogu pojednostaviti procedure vezane za rezervisanje mesta, predaju prtljaga i slično
  - Elektronske karte i vaučeri mogu pružiti i dodatni komfor koji do sada nije bilo moguće obezbediti
  - Smart kartice mogu poslužiti i pri naplati putarine, parkinga itd.
- **Zdravstvo**
  - Smart kartica može poslužiti kao zdravstvena knjižica i zdravstveni karton
  - Na njoj mogu biti smešteni podaci koji mogu biti od životne važnosti u hitnim slučajevima – koja je vlasnikova krvna grupa, na šta je alergičan, da li je srčani bolesnik itd.
  - Mogu se čuvati i podaci o korisnikovom zdravstvenom osiguranju