



Elektronsko Bankarstvo:

Lekcija 9: Sistemi plaćanja preko Interneta (I)

2018/2019

Branimir M. Trenkić

Sistemi plaćanja - Uvod

(Iz predhodne lekcije (Lekcija 7)):

- Modeli plaćanja preko Interneta – elektronske verzije modela u tradicionalnim sistemima plaćanja:
 - Ček,
 - Keš (gotovina),
 - Platne kartice,
 - Platni nalog.
- Osnovna razlika – elektronski sistemi plaćanja su u potpunosti elektronski i digitalni

Sistemi plaćanja - Uvod

- Treba *praviti razliku* između elektronskog plaćanja i elektronske transakcije
 - *Elektronsko plaćanje* – transferisanje novca
 - *Elektronska transakcija* – uključuje: isporuku, *plaćanje*, potvrdu plaćanja, potvrdu prijema narudžbenice,
 - *Sistem plaćanja* – predstavlja samo deo interakcije sa servis provajderom
- *Sistem elektronske trgovine* – mora da *implementira* i *ostale delove el. transakcija*

Sistemi plaćanja - Zahtevi

- **Glavni problem** plaćanja preko Interneta – **nedostatak bezbednosti**
- **Dve grupe učesnika** u elekt. transakcijama koji imaju **slične zahteve po pitanju sigurnosti**:
 - **Kupci** i **trgovci**
 - Gotovo **iste želje i strahove** u pogledu **mehanizama elektronskog plaćanja**
 - **Finansijske intitucije** i zakonska **regulatorna tela**
 - Obezbeđuju usluge za izvršenje transakcije i imaju svoje zahteve u pogledu mehanizama plaćanja

Sistemi plaćanja - Zahtevi

Kupci i trgovci

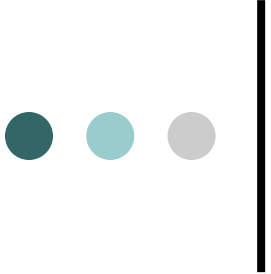
○ **Bezbednost**

Elektronski novac je samo **podatak** – koji se može jednostavno kopirati!

- **Obezbediti sigurnost** da niko ne može preusmeriti plaćanje ili **se predstaviti kao druga osoba**
- Nijedan učesnik u sistemu ne mora da veruje drugom učesniku

○ **Prihvatljivost**

- **Široki opseg učesnika** treba da **prihvati određeni metod plaćanja**



Sistemi plaćanja - Zahtevi

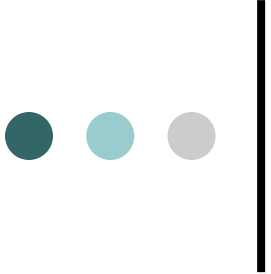
Kupci i trgovci

○ **Pogodnost**

- Odnosi se na
 - ***napore koje učesnik treba da uloži***
 - ***brzinu procesuiranja*** transakcije

○ **Troškovi**

- Poželjno je da transakcije ***ne iziskuju dodatne troškove***
- ***Transakcioni troškovi*** uključuju ***direktne troškove***: kupaca, trgovaca, posrednika + troškovi obrade transakcije



Sistemi plaćanja - Zahtevi

Kupci i trgovci

- **Privatnost**

- Za razliku od plaćanja gotovim novcem – kod elektronskog plaćanja ***to najčešće nije slučaj***

- **Izdržljivost (robustnost)**

- Elektronski novac ***ne bi smeo lako da se izgubi*** (npr. usled pada sistema na računaru)

Sistemi plaćanja - Zahtevi

Finansijske institucije i regulatorna tela

○ ***Trenutna kontrola***

- Svaka transakcija se ***pojedinačno prati*** – tako da se bezbedonosni ***napad može vrlo brzo uočiti***

○ ***Mogućnost praćenja***

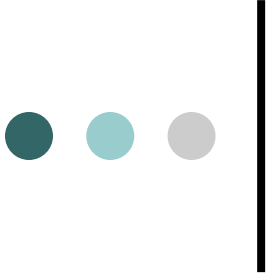
- Omogućeno ***praćenje transakcija*** – ako se uoči zloupotreba, ***počinilac se može identifikovati***

○ ***Kontrola korišćenja mehanizama enkripcije***

- Ključna ***briga vlade i regulatornih tela***

Sistemi plaćanja - Zahtevi

- Mnogi od ovih zahteva je **međusobno kontradiktorno** – ne mogu se istovremeno realizovati u sistemu plaćanja
- Npr. **želja za anonimnosti** i privatnosti i **želja posrednika da može da uđe u trag izvršenim transakcijama**
 - Tradicionalni **posrednici** – **banke**
 - **Sistemi bez anonimnosti** - Naglašavaju želju korisnika da **prate** svoje **vlastite transakcije**
 - Postoje i sistemi koji poseban **naglasak** stavljaju **na anonimnosti korisnika**



Sistemi plaćanja - Podela

- Svi **sistemi plaćanja** se mogu klasifikovati u dve kategorije:
 - 1) Sistemi zasnovani na **bankovnom računu**
 - 2) Sistemi zasnovani na **tokenima**
- **Glavna razlika** – u omogućavanju anonimnosti

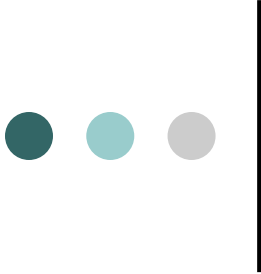
Sistemi plaćanja - Podela

○ *Korišćenje platnih kartica*

- Trenutno *najpopularniji način plaćanja preko Interneta*
- Sistem *zasnovan na računu* – banka jednostavno može da vidi *koliko* plaća korisnik, *kome*, *kada* i *gde*
- *Omogućava se profiliranje korisnika* na osnovu njegovih *potrošačkih navika* - matematička tehnika - *data mining (rudarenje)*

Sistemi plaćanja – Kriterijumi uspeha

- **Uslovi** potrebni **za uspeh** nekog sistema plaćanja
 - a) Potrebno je da **svi korisnici sistema ostvare korist** od njegovog korišćenja
 - **Korist** svakog učesnika **veća od troškova i rizika** kojim su izloženi
 - b) Da sistem **dostigne kritičnu masu učesnika** (i kupaca i trgovaca)
 - Glavni razlog neuspeha prve generacije sistema
 - Glavni razlog uspeha **PayPal kompanije**
 - **Savez sa eBay** omogućio je **pristup kritičnoj masi korisnika**



Sistemi plaćanja - Kriterijumi uspeha

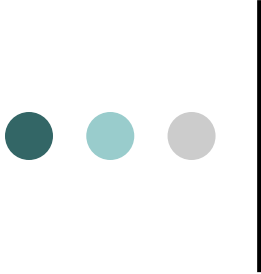
c) *Rešiti određene bezbedonosne probleme* koji nastaju prilikom *slanja elektronskog novca* preko *otvorenih mreža*:

- a) Poverljivost
- b) Autentifikacija
- c) Očuvanja integriteta
- d) Ne-poricanja transakcije
- e) **Anonimnost**
- f) **Sprečavanje dvostrukog trošenja novca**

a), b), c), d):

Digitalni potpis:

Rešava problem
falsifikovanja novčanica

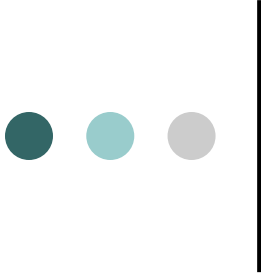


Sistemi plaćanja - Kriterijumi uspeha

- Sistemi elektronskog plaćanja treba **da otkriju i onemoguće dvostruko (višestruko) trošenje** elektronskog **novca**

1. način

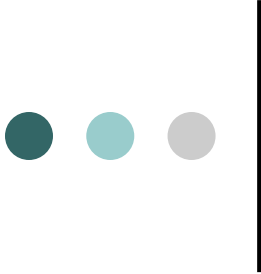
- Potrebna je **komunikacija trgovca sa bankom** u **svakoj transakciji**
- U **bazi podataka banke** nalaze se **informacije o utrošenom** elektronskom **novcu** – kako bi se jednostavno otkrio novac koji je već potrošen
- Ako računar otkrije ovakav novac – obaveštava trgovca



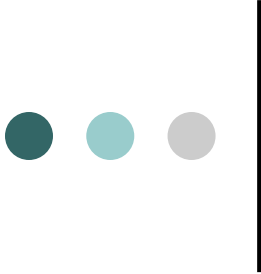
Sistemi plaćanja - Kriterijumi uspeha

2. način

- **Korišćenje smart kartice** – koja sadrži čip sa mini bazom podataka sa *podacima o svim utrošenim tokenima*
- Ako **korisnik pokuša da kopira neki novac** kako bi ga dva puta potrošio – **čip** će otkriti ovaj pokušaj i **neće dozvoliti transakciju**
- Korisnik ne može da izbriše ovu mini bazu

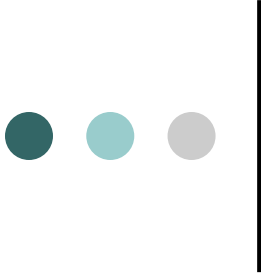


Sistem plaćanja – Platne kartice



Sistem plaćanja – Platne kartice

- U standardnim transakcijama:
- **Kupac** daje preliminarne **dokaze o svojoj platežnoj sposobnosti** – prezentujući trgovcu broj svoje platne kartice
- **Trgovac** ovo **može da verifikuje kod banke** izdavaoca platne kartice
- **Nakon toga** se vrši **prenos sredstava** sa računa kupca na račun trgovca
- **Kupac** dobija **od banke potvrdu o izvršenom transferu**

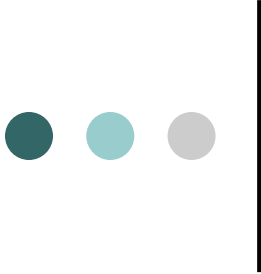


Sistem plaćanja – Platne kartice

- ***Plaćanje platnom karticom preko Interneta – sličan scenario***
- Potrebni su ***dodatni koraci*** u cilju ***obezbeđenja sigurne transakcije***
- Razvijeni su ***različiti sistemi*** za korišćenje platnih kartica preko Interneta – ***razlikuju se po nivou sigurnosti***
- ***Moguće je slanje neenkriptovanih*** ili ***enkriptovanih podataka*** sa platne kartice
- ***U prvom slučaju – nema bezbedonosnih garancija***

Sistem plaćanja – Platne kartice

- ***U slučaju enkriptovanih*** podataka
- ***Trgovac*** mora da ***dekriptuje podatke*** koji se ***tiču narudžbine***
- ***Treća poverljiva strana*** se koristi za ***dekriptovanje podataka sa platne kartice*** u cilju obavljanja ***autorizacije narudžbine***
- U cilju ***obezbeđivanja sigurne komunikacije*** preko Interneta – ***koriste se sigurnosni protokoli*** (kao što su ***SSL*** ili ***SET***)



Sistem plaćanja – Platne kartice

- Korišćenjem **servera** i **pretraživača** koji ***podržavaju ove protokole*** – **štite se podaci** od mrežnog nadgledanja i špijuniranja
- **Ne garantuje se zaštita podataka na strani trgovca**

Platne kartice – SSL protokol

Učesnici

- Kupac koji *poseduje platnu karticu*
- Finansijska institucija koja je *izdala karticu*
(vrši autorizaciju transakcija)
- Trgovac koji ima:
 - Svoj *veb sajt*
 - *Račun u banci* (merchant account) koji omogućuje prihvatanje *plaćanja sa platne kartice*
- Posrednik pri plaćanju – **TGP** (Transaction Gateway Provider)

● ● ● | Platne kartice – SSL protokol

Koraci u procesu plaćanja

- **Kupac** **posećuje veb sajt trgovca** i u **virtuelnu potrošačku korpu** stavlja proizvode koje želi da naruči
- **Odlazi na zaštićenu stranu (SSL)**, **unoseći** svoje lične podatke, adresu isporuke, **podatke** koji se **tiču plaćanja pomoću platne kartice**
- Kada su svi podaci uneti **klikom na dugme**, **kupac** ih **prosleđuje** ka **serveru trgovca**
- **Na serveru** se nalazi specijalni softver (dobijen od TGP-a), koji **podatke šalje ka TGP-u**

Platne kartice – SSL protokol

Koraci u procesu plaćanja

- **TGP** uz posredstvo **banke** **vrši autorizaciju transakcije** – proverava da li kupac ima dovoljno novca na računu, ili da li je dovoljno kreditno sposoban ako se radi o kreditnoj kartici
- Ukoliko je **autorizacija uspešna** – **potvrdu o tome TGP prosleđuje trgovcu**
- **Kupčeva banka transferiše sredstva sa računa kupca na račun trgovca**

Platne kartice – SSL protokol

- Problem – *bezbednost na strani servera*
- *Brojevi platnih kartica* se prosleđuju do servera trgovca – postoji mogućnost da *trgovac odluči da ih sačuva u bazi podataka*
- Na ovaj način se stvara *mogućnost neautorizovanog korišćenja* brojeva platnih kartica

Platne kartice – SET protokol

- Trgovac – na osnovu provere identiteta i platne sposobnosti – *otvara račun kod banke*
- I *dobija*:
 - a) **SET softver** za obavljanje plaćanja
 - *Integriše ga u svoj veb sajt*
 - b) **Digitalni sertifikat** (koji ga jedinstveno identifikuje)

Platne kartice – SET protokol

- **Kupac** - na osnovu provere identiteta i platne sposobnosti – **dobija digitalnu platnu karticu**
- Ova **kartica predstavlja** njegov **digitalni sertifikat**
- Potrošač je stavlja u **“browser wallet”** – **aplikaciju za veb pretraživač**
- Pomoću nje **kupac prosleđuje enkriptovani broj platne kartice** sa **digitalnim potpisom do trgovca**

Platne kartice – SET protokol

- Trgovac - je *sprečen da vidi* i neautorizovano koristi *broj platne kartice kupca*
- SET softver na njegovom sajtu – *šalje transakciju do procesora platnih kartica* (tzv. gateway aplikacije za plaćanje)
- Procesor - tu se *podaci dešifruju, obrađuju i verifikuju* uz pomoć CA
- Zatim, *šalje transakciju do banke* koja je izdala platnu karticu

Platne kartice – SET protokol

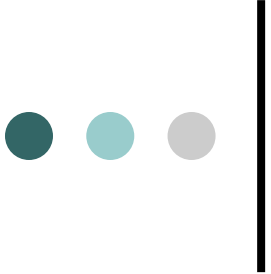
- Banka – (koja je izdala platnu karticu) **poseduje SET softver** *radi* obavljanja **autorizacije**
- Trgovac - elektronski **dobija potvrdu da je narudžbina odobrena** i da je račun vlasnika platne kartice zadužen – tek tada **izvršava isporuku robe** (ili usluge)

Platne kartice – SET protokol

- Da bi **SET protokol postao** (default) **standard** za bezbedno plaćanje preko Interneta – neophodno je bilo **da se prevaziđu neke prepreke**
- Potrebno je bilo postići **interoperabilnost** između raznih proizvođača softvera
- IBM, Verifone, SETco,.... – zajedno su **radili na uspostavljanju standarda** što se tiče SET protokola
 - Trebalo je **da omogući mnogo bezbedniju** ²⁹**transakciju plaćanja** preko Interneta

Platne kartice – SET protokol

- Pri tom bi trebalo **omogućiti sledeće**:
- **Da kupci** pomoću **svog veb pretraživača** mogu **da obavljaju transakcije sa bilo kojim trgovcem** na Internetu,
- **Da** bilo koji **gateway procesor** obavi transakciju od **bilo kog trgovca**,
- **Da** bilo koja **SET komponenta** dobije **SET sertifikat od bilo kog SET sertifikacionog tela**



Platne kartice – SET protokol

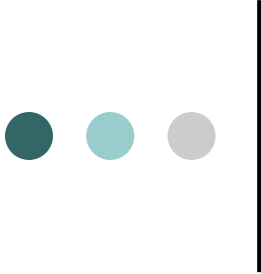
- *SET je* predstavljao *idealno rešenje* za enkripciju
- Vršio je *autentifikaciju svih učesnika*
- Obezbeđivao *poverljive podatke*
- Vršio *proveru integriteta poruke*

Platne kartice – SET protokol

- **SSL je manje savršen** – jer se kupac ne autentifikuje
- Zbog toga, se **transakcije sa platnim karticama zasnovane na SSL-u** klasifikuju **od strane izdavaoca kartice** kao **“korisnik kartice nije prisutan”** plaćanje

Platne kartice – SET protokol

- Klasifikacija “**korisnik kartice nije prisutan**” znači da *u slučaju krađe* – odštetu plaća trgovac a ne kompanija koja je izdala karticu
- **Trgovac** ovo *amortizuje velikim brojem transakcija* koje ostvaruje
- **SSL se**, za razliku od SET protokola koji je napušten od svojih kreatora – *i dalje uspešno koristi*



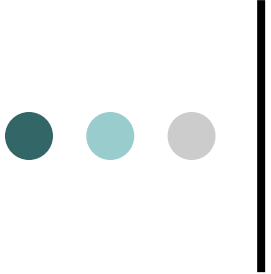
Prvi platni sistemi na Internetu

- ***Prve kompanije*** (platni sistemi na Internetu)
- Započele su sa radom ***90-tih godina*** prošlog veka
- ***First Virtual***,
- ***Verifone*** i
- ***CyberCash***

First Virtual



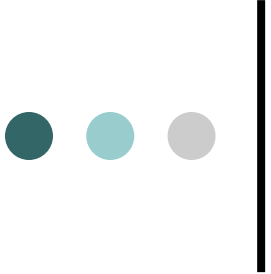
- *Jedan od prvih sistema plaćanja na Internetu*
- *Jednostavan* sistem za korišćenje
 - Od korisnika *ne zahteva nikakvu dodatnu instalaciju softvera*, i
 - *Jedini uslov pristup Internet e-mail servisu*
 - Jedinstven u smislu da *ne koristi enkripciju*
- *Osnovna zamisao* - *podaci* koji su *bitni* radi sigurnosti *ne treba da idu kroz mrežu*
- Da bi se koristio ovaj sistem – obavezna je *registracija korisnika*



First Virtual

Registracija korisnika

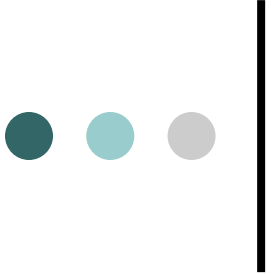
- *First Virtual* – **izdaje korisnicima VirtualPIN**
(lični identifikacioni broj, **FV PIN**)
- Taj kod **kupci** kasnije **koriste umesto broja platne kartice**
- Korisnik mora **prilikom registracije** da unese svoje podatke:
 - **Platna kartica** (Visa, MasterCard, ...)
 - **e-mail adresa** korisnika
 - ...³⁶



First Virtual

Proces kupovine i plaćanja se odvija kroz sledeće korake:

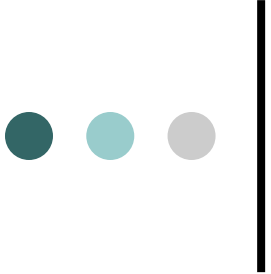
- **Na sajtu trgovca kupac** pronalazi traženu robu i **unosí** svoj **FV PIN**
- **Trgovac proverava** FV PIN (opciono!)
 - Primenom sledećih programa: *Finger*, *Telnet*, ili *FV_API utility*
- **Trgovac inicira transakciju** plaćanja preko FV **šaljući** mu sledeće podatke:
 - **FV PIN trgovca**, **FV PIN kupca**, **iznos**, **valuta**, **opis proizvoda**



First Virtual

Proces kupovine i plaćanja se odvija kroz sledeće korake:

- *First Virtual šalje e-mail poruku kupcu* na koju on treba da odgovori i *potvrdi kupovinu*. Ova poruka u sebi sadrži sledeće informacije:
 - *ime trgovca, iznos, opis proizvoda*
- *Kupac potvrđuje* sa da ili ne, prihvata li kupovinu ili je odbija. To radi *putem e-mail* pošte. Ukoliko ne odgovori u nekom zadatom roku *transakcija se poništava*

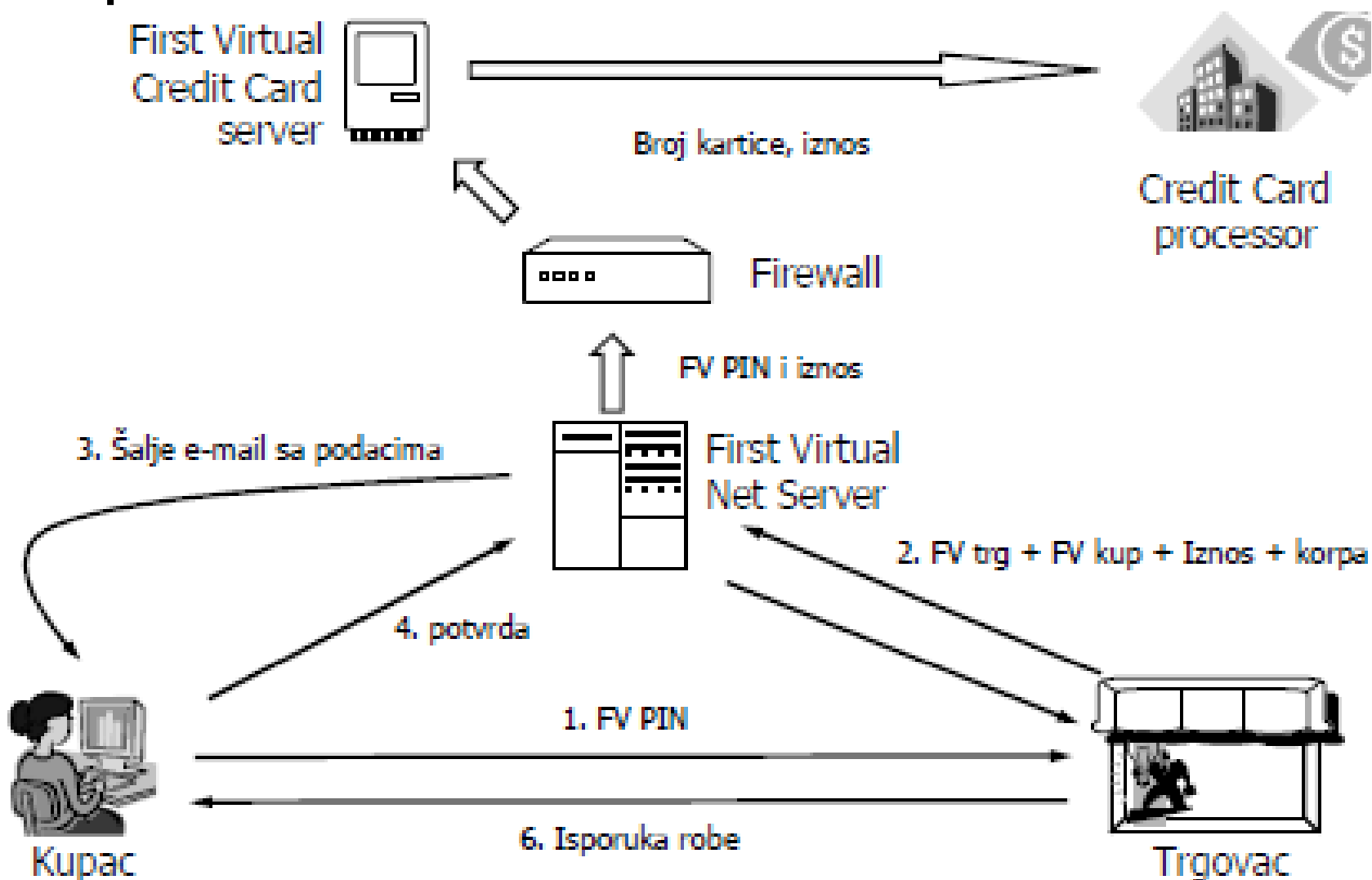


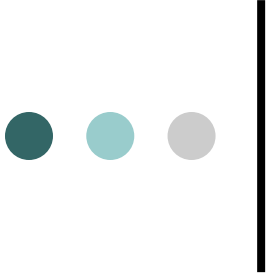
First Virtual

Proces kupovine i plaćanja se odvija kroz sledeće korake:

- *First Virtual šalje poruku trgovcu da je **prodaja prihvaćena** i da će nakon 91-og dana novac biti uplaćen na njegov račun*
 - Iznos **umanjen za troškove transakcije**

First Virtual





First Virtual

- **Najveći problem** ovog sistema – **rok isplate** sredstava
- U savremenom poslovanju, gde se obrt novčanih sredstava meri satima i danima – **rok za povraćaj sredstava od 91 dana je isuviše dug**
- **Dobra strana** ovog sistema – **ni kupac ni prodavac nemaju potrebe za dodatnim softverom**
 - Kupac je zaštićen od prevare
 - **Kupovina je anonimna**

CyberCash



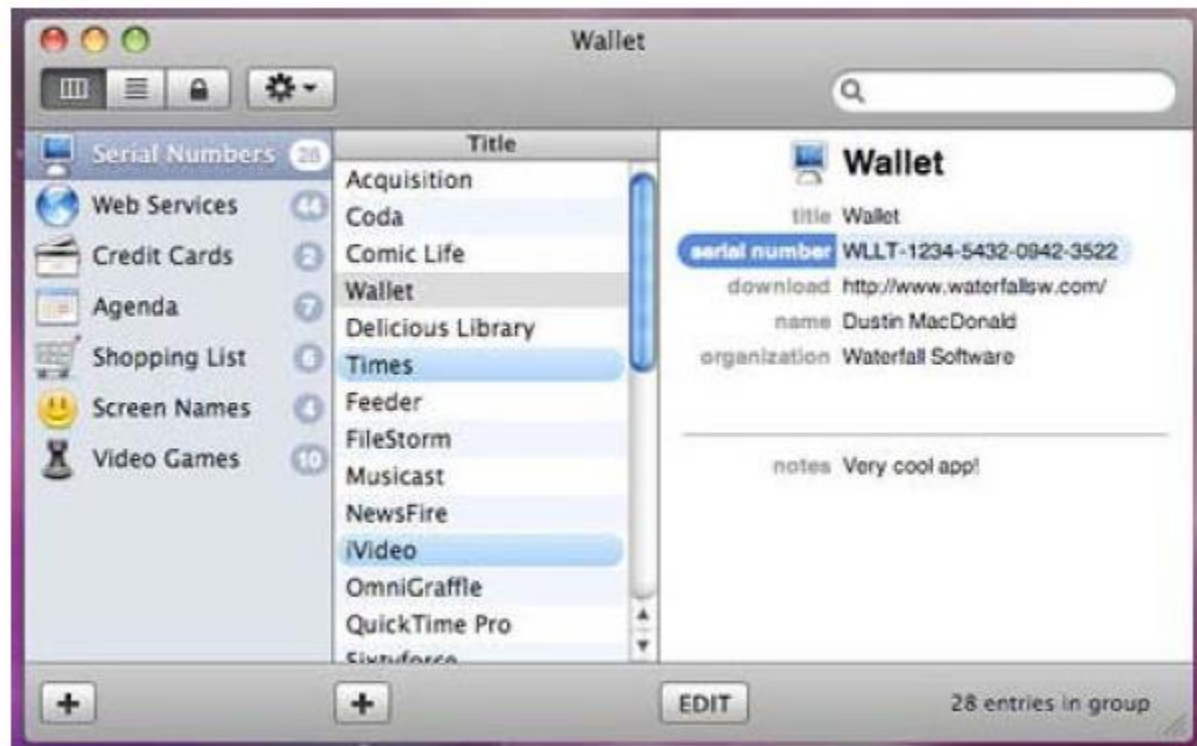
- Kompanija **osnovana 1994. godine** – bila je **vodeća** u **on-line sistemima plaćanja**
- Koristi (**između ostalog**) **tehnologiju platne kartice** za plaćanje preko Interneta
- Daje trgovinama i kupcima **softver koji emulira POS proces** u realnom sistemu plaćanja pomoću platne kartice
- **Kupac mora da ima** instaliran **program CyberCash Wallet** – služi kao pomoćna **aplikacija za veb pretraživač**

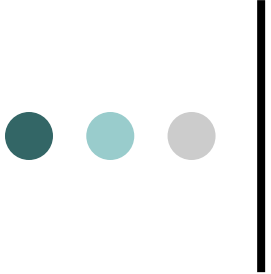
CyberCash

Primeri *programskog paketa* **Wallet**

Qwallet:

Wallet (za Mac):

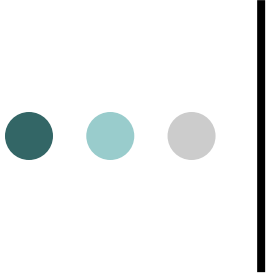




CyberCash

Registracija - kupac

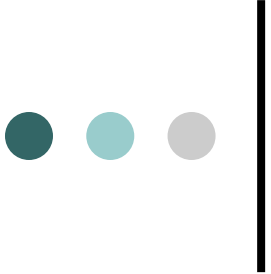
- Preduslov: **Kupac mora da ima** instaliran **program CyberCash Wallet**
 - Ovaj program upravlja **slanjem informacija za plaćanje, enkripcijom**, između kupca i prodavca
- **Kupac kreira wallet ID i lozinku** svog CyberCash Wallet-a i **registruje ih** kod CyberCash-a kako bi mogao **da obavlja kupovinu** pomoću ovog sistema
- Kupac mora **bar jednu platnu karticu** povezati sa ⁴⁴CyberCash Wallet-om



CyberCash

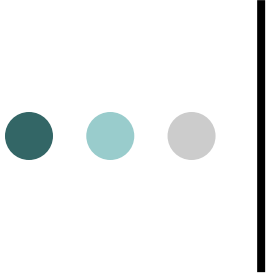
Registracija - trgovac

- Preduslov: ***Trgovac mora da ima*** instaliran program ***CyberCash Internet Payment Software***
 - Ovaj program omogućuje **interfejs** sa kupcem (***CyberCash Wallet***) s jedne strane i ***CyberCash serverom*** s druge strane
- Trgovac mora ***otvoriti račun u banci*** koja **podržava** Internet transakcije korišćenjem CyberCash Internet Payment System



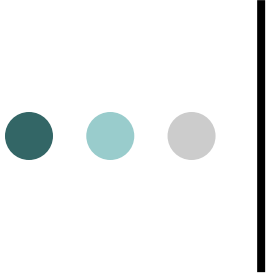
CyberCash

- Kada **kupac klikne na dugme za plaćanje** na sajtu trgovca – **informacija** se **prosleđuje do CyberCash- servera** koji je nevidljiv za korisnika
- **CyberCash server** je povezan na postojeće **mreže banaka** radi validacije transakcije
- **CyberCash server prosleđuje trgovčevoj banci na obradu podatke** koje dobija od trgovca



CyberCash

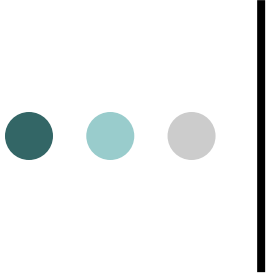
- Banka komunicira sa trgovcem preko CyberCash servera
- ***Transakcija se obrađuje na isti način kao da je zahtev primljen preko POS terminala***



CyberCash

Proces kupovine i plaćanja se odvija kroz sledeće korake:

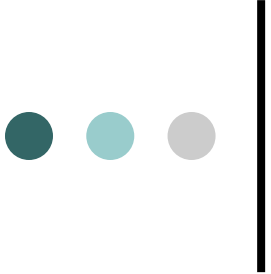
- **Kupac** signalizira da *hoće da plati*
- **Trgovac** šalje *fakturu* na *kupčev Wallet*
- **Kupac bira** neku od platnih *kartica koje ima u* digitalnom *novčaniku*
- **Kupčev Wallet** digitalno *potpisuje i šifrira* *fakturu*, i *informacije* koje su unete *o platnoj kartici*



CyberCash

Proces kupovine i plaćanja se odvija kroz sledeće korake:

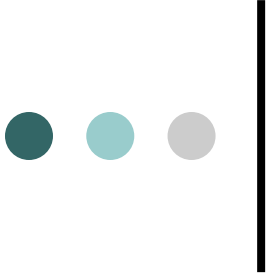
- **Trgovac** prima ovako **šifriran paket** i dodaje svoj **zahtev za obradom plaćanja**
- Takođe **stavlja svoj digitalni potpis** (**dobra strana ovog sistema** je što **trgovac nikada nije u mogućnosti da vidi broj platne kartice**)



CyberCash

Proces kupovine i plaćanja se odvija kroz sledeće korake:

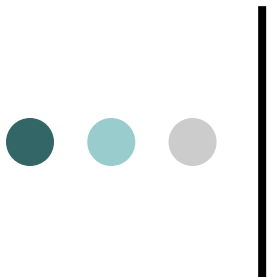
- **Cyber Cash** *prebacuje* paket na računar i *dekriptuje poruku*
- **Podaci za banku** se *posebno kriptuju* i prosleđuju se *trgovčevoj banci* a ona prosleđuje podatke *banci* koja je *izdala karticu*



CyberCash

Proces kupovine i plaćanja se odvija kroz sledeće korake:

- **Izdavaoc kartice** dalje **skida sa računa** i **šalje** odobrenje sa podacima o završenoj transakciji
- **Cyber Cash** **prosleđuje** podatke **trgovcu** (**sve se odvija u roku od 20 sekundi**)
- **Trgovac** šalje **kupcu** **potvrdu** da je **transakcija uspešno sprovedena** i **dostavlja mu** **broj** **pod kojim je transakcija izvršena**



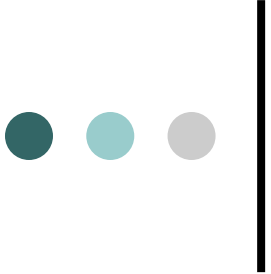
Elektronski čekovi

Elektronski čekovi

- **Elektronski ček** ili e-ček **se zasniva na ideji**
 - da **elektronski dokument** može **da zameni papirni** dokument i
 - da **kriptografski potpis** može **da zameni ručni** potpis
- **Ček** – **poruka kupčevoj banci** da izvrši **transfer fondova** sa računa kupca na račun trgovca

Elektronski čekovi

- **Kupac koji plaća e- čekom** digitalno potpisuje obrazac (el. dokument) koji sadrži
 - Opis transakcije
 - Informacije o platiocu i primaocu
 - Iznos
 - Vremenski žig – kombinacija datuma i vremena odigravanja transakcije
- **Broj računa može biti zaštićen** od zloupotrebe kodiranjem bančnim javnim ključem – što e-ček čini superiornijim od papirnog čeka



Elektronski čekovi

Proces kupovine i plaćanja se odvija kroz sledeće korake:

- *Kupac* i *trgovac* se *pronalaze na Internetu* i kupac *formira korpu za plaćanje*
- *Trgovac* formiranu korpu *formatira u oblik fakture* i *prosleđuje* na kupčev računar
- Na *kupčevom računaru* se nalazi softver koji *prihvata fakturu i započinje proces* plaćanja čekom

Elektronski čekovi

Postupak rada sa elektronskim čekovima:

- Prilikom **startovanja softvera** za rad sa elektronskim čekovima **na ekranu se pojavljuje slika elektronskog čeka**

If paying by electronic check, please fill out the fields below:

Name on account:

Name of bank:

Type of Account: 

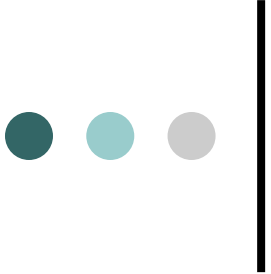
Check Number:

Routing Number Account Number

Important note: Do not click this button more than once.
It may take up to 30 seconds for our payment processor to respond.

[Continue...](#)



Elektronski čekovi

Postupak rada sa elektronskim čekovima:

- Ček na ekranu je prethodno pripremljen ***i ima izgled i formu papirnog čeka***
- ***Kupac popunjava podatke:*** **datum**, **kome** treba da bude isplaćen ček (naziv primaoca) i **iznos** koji treba da se isplati
- Time su kompletirani podaci i ***ček treba potpisati***

Elektronski čekovi

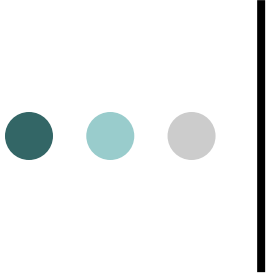
Postupak rada sa elektronskim čekovima:

- **Potpisivanje čeka** je *pomoću smart kartice*
 - Smart kartica se ubacuje u uređaj za čitanje i **unosí se PIN broj** da bi se **otključala kartica**
 - **Serijski broj čeka** se *automatski dodaje iz Smart kartice*
 - Na kraju **kartica čita sve podatke** sa čeka i **formira digitalni potpis**
 - Nakon toga ček se **pakuje u digitalni koverat** i šalje trgovcu
- Ovako pripremljen ček se šalje kao bilo koji e-mail

Elektronski čekovi

Postupak rada sa elektronskim čekovima:

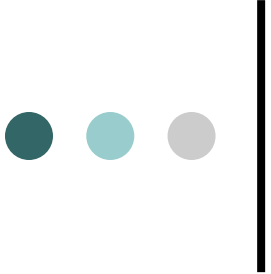
- **Trgovac prihvata** ovako pripremljen **ček** na svom računar
- Softver **skida deo** koji se **odnosi na narudžbenicu** i **potpisuje ček** dodajući svoj **digitalni sertifikat**
- Ovako obrađen ček **trgovac šalje svojoj banci** na naplatu
- **Dalji postupak** je isti kao kod bilo kog drugog čeka



Elektronski čekovi

Postupak rada sa elektronskim čekovima:

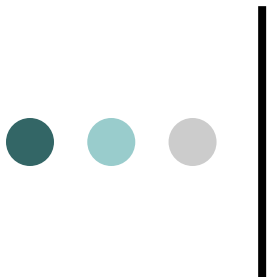
- ***Svaki izdat ček*** može biti ***sačuvan na računaru*** kao verna kopija originala
- Samo ***jedna kopija*** čeka ***može biti plaćena*** jer postoji ***kontrola i detekcija duplikata***
- ***Kopije mogu biti sačuvane na više mesta***, čak mogu biti i ponovo kopirane i distribuirane bez ikakvih posledica



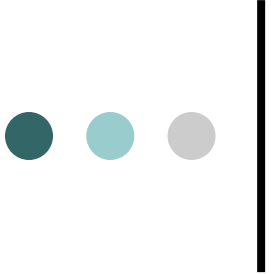
Elektronski čekovi

Postupak rada sa elektronskim čekovima:

- ***Digitalni potpis*** na e-čeku može biti ***proveren u svakom trenutku***
- Takođe se ***može izvršiti autentifikacija potpisnika*** e-čeka a on ni sam ni na koji način ne može biti modifikovan ili falsifikovan



Digitalni keš

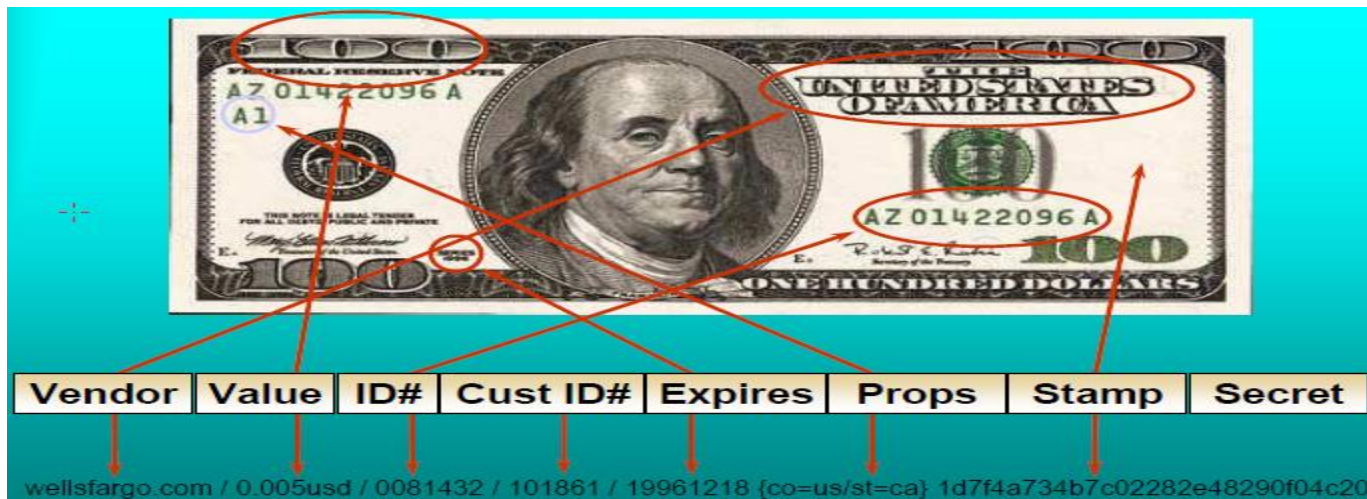


Digitalni keš

- **Sistemi koji se baziraju na digitalnom kešu** (**e-gotovina**) - **najbolje se uklapaju** u mogućnost obavljanja transakcija koje uključuju **male novčane iznose** – **mikro plaćanja**
- Može biti **izdat u veoma malim apoenima** (**mikrotransakcije**)

Digitalni keš

- **Digitalni keš** - u formi validiranih tokena – niz cifara (karaktera) koje izdaje i otkupljuje banka
- Banka validira svaki token digitalnim potpisom pre izdavanja korisniku
- **Račun korisnika** se zadužuje za vrednost izdatih tokena

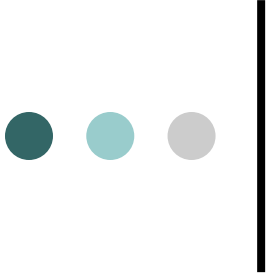


Digitalni keš - Plaćanje

- Kupac *plaća digitalnim kešom prebacivanjem* odgovarajućeg iznosa *tokena trgovini*
- Trgovina ih zatim *prosleđuje banci* radi verifikacije i otkupa
- Banka *evidentira serijski broj* svakog potrošenog tokena – da bi bila sigurna da je *token korišćen samo jedanput*
- Ako je *serijski broj već zapisan* u BP banke izdavaoca – banka obaveštava trgovca da je *token bezvredan*

Digitalni keš – Nedostatak

- **Digitalni keš** može biti izdat **u veoma malim apoenima**, tzv. mikro-keš
- Koristi se za **plaćanje sitnih transakcija** (iznajmljivanje softvera, on-line igrice,...)
- Međutim, **troškovi provere autentičnosti** svakog tokena su **relativno visoki** – što dovodi u pitanje **pogodnost ovog sistema** za mikroplaćanja



Digitalni keš

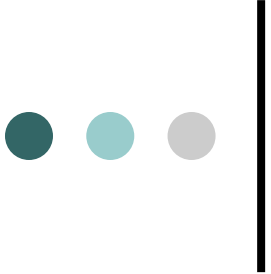
- Postoji **više sistema za mikroplaćanja**
- **Prva generacija** sistema
 - Pojavila se **1994. godine**
 - *CyberCash, DigiCash, E-cash,*
- **Druga generacija** sistema
 - **Početakom 21. veka**
 - *Wallie, Peppercoin, Clic&Buy, Micromoney, PaySafeCard,*

Slepi potpis

- Slepi potpis uveo je *David Chaum* kao **oblik** digitalnog **potpisivanja dokumenta** bez uvida ili sa delimičnim uvidom u sadržaj dokumenta
- **Potpuno slepi potpis** ne daje nikakav uvid u sadržaj dokumenta
- **Digitalno potpisivanje** poruke - moguće je samo ako potpisnik ima pristup izvornoj poruci
- U situacijama kada **potpisnik ne sme videti originalnu poruku** koju potpisuje, primenjuje se slepi digitalni potpis

Slepi potpis

- Slepi digitalni potpis razlikuje se od običnog digitalnog potpisa u tome što se pre potpisivanja originalna poruka "prikriva"
- Tehnike "prikrivanja" mogu biti različite
 - Npr. množenjem brojem r (**faktor slepoće**) – nastao kombinacijom slučajnog broja i javnog ključa banke
- Nakon potpisa privatnim ključem banke - poruka se "otkriva" deljenjem sa slučajnim brojem r



Slepi potpis

- Sada je faktički *poruka* samo potpisana privatnim ključem banke
- Ovo je *moгуće* zato što su *funkcija prikrivanja* i *funkcija potpisivanja* komutativne

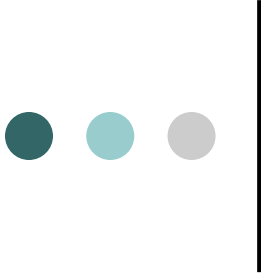
Slepi potpis

- Analogija potpuno slepom potpisu bilo bi potpisivanje na dokument koji se ***zajedno sa indigo-papirom*** nalazi u koverti
 - Osoba se potpisuje preko koverte i indigo-papira na dokument, ali ***ne može pročitati*** dokument
- Takvo potpisivanje je obično ***rizično*** - pogotovo za banku
 - Treba ***da potpiše elektronsku novčanicu***, a ***ne zna na koji iznos glasi*** ta novčanica
- Zato se uvodi ***slepi potpis s delimičnim uvidom*** u sadržaj dokumenta

Slepi potpis

- Protokol slepog potpisivanja sa delimičnim uvidom:

1. Osoba A priprema n digitalnih **novčanica iste nominalne vrednosti**, ali **drugačijih serijskih brojeva** - prikrivene faktorom slepoće šalje ih banci (svaka novčanica – jedinstven faktor slepoće)
2. Banka **proverava sadržaj** slučajno odabranih $n - 1$ **novčanica** zahtevajući od osobe A da ih “otkrije” - prosledi faktore slepoće za te novčanice



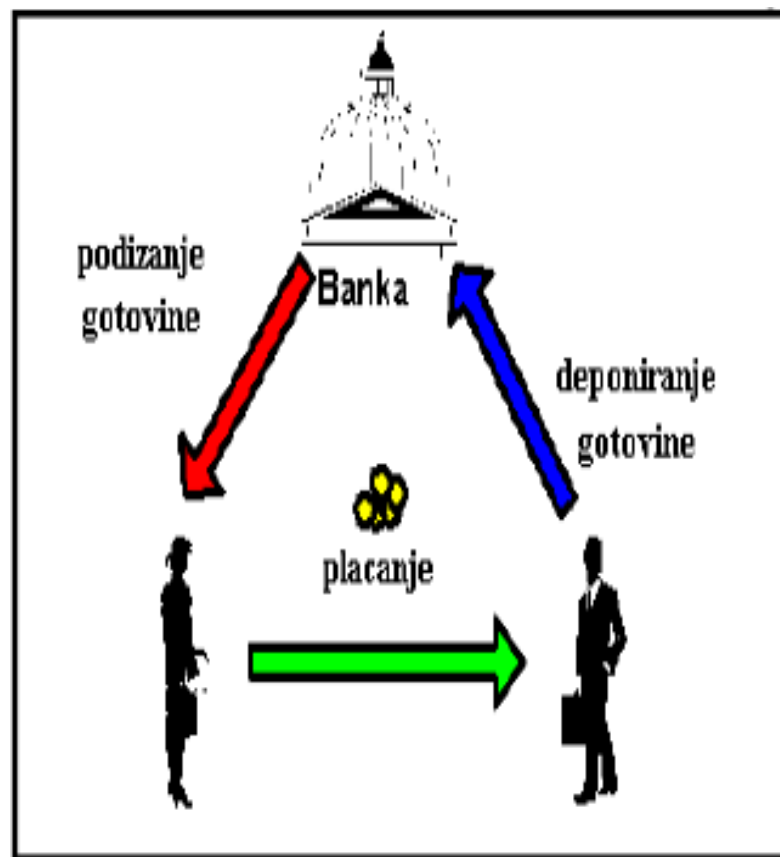
Slepi potpis

- Protokol slepog potpisivanja sa delimičnim uvidom:
- 3. Ako su **sve otkrivenene novčanice valjane**, **banka potpisuje preostalu neotkrivenu novčanicu** (čiji serijski broj nije u mogućnosti videti) i **vraća je osobi A**

Protokol bez anonimnosti

- **Proces plaćanja**, odnosno kupovine se može **podeliti u tri faze**:

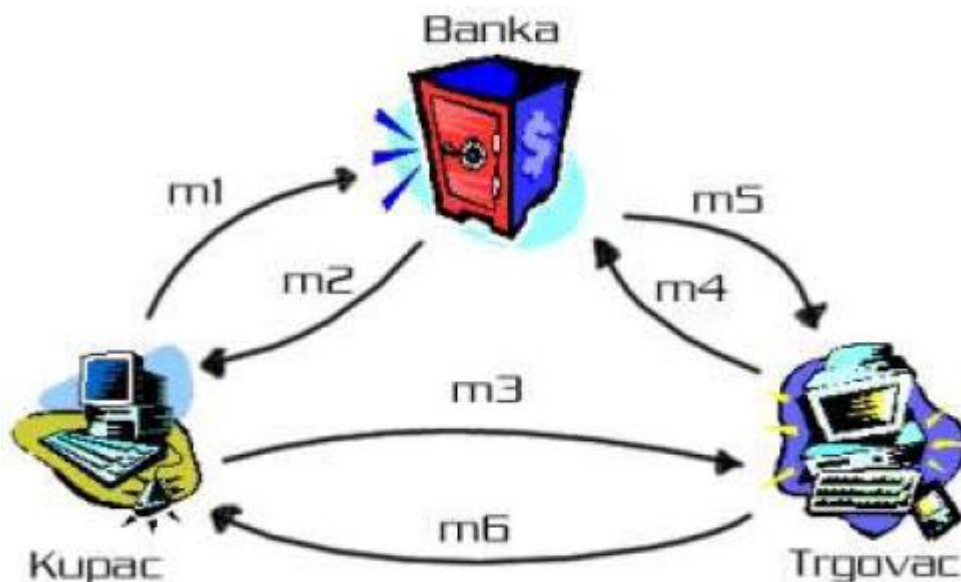
1. **Podizanje** novca iz banke
2. **Plaćanje**
3. **Polaganje** novca u banku



Protokol bez anonimnosti

Podizanje novca iz banke:

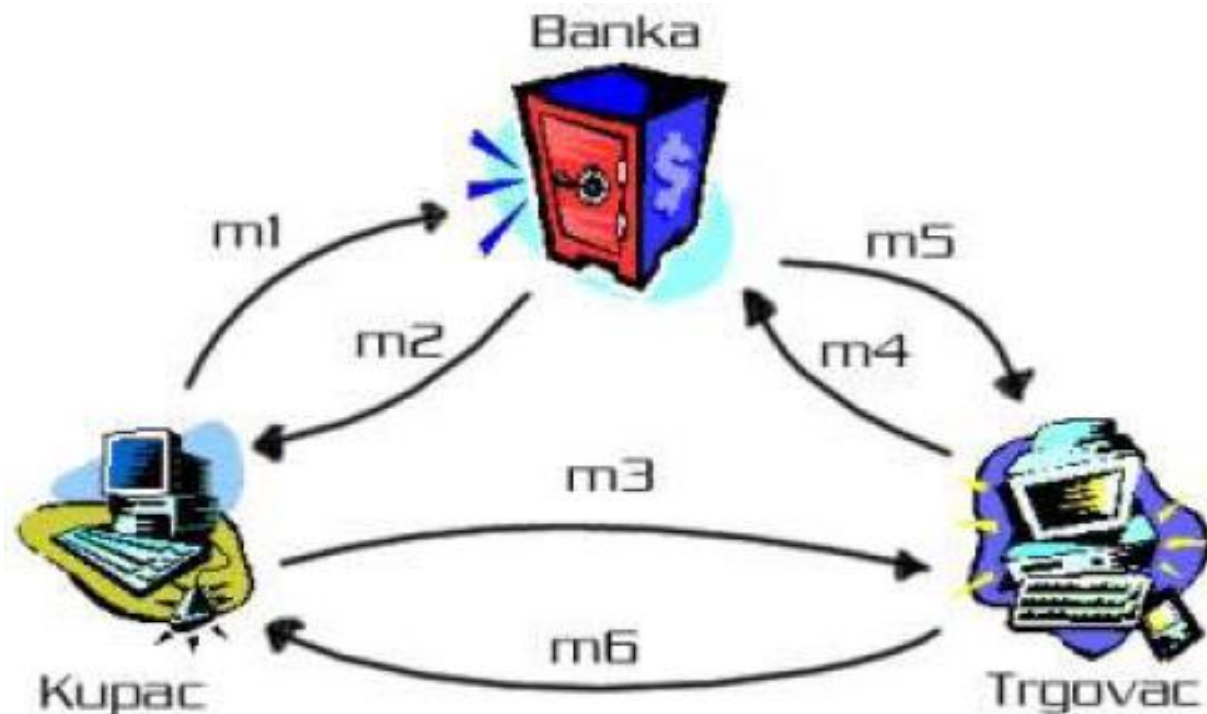
- **kupac** šalje zahtev banci za određenom količinom elektronskog novca (**m1**);
- **banka** oblikuje elektronsku novčanicu (sa serijskim brojem) i **stavlja digitalni potpis**;
- **banka šalje** elektronsku novčanicu kupcu i umanjuje njegov račun (**m2**)



Protokol bez anonimnosti

Plaćanje:

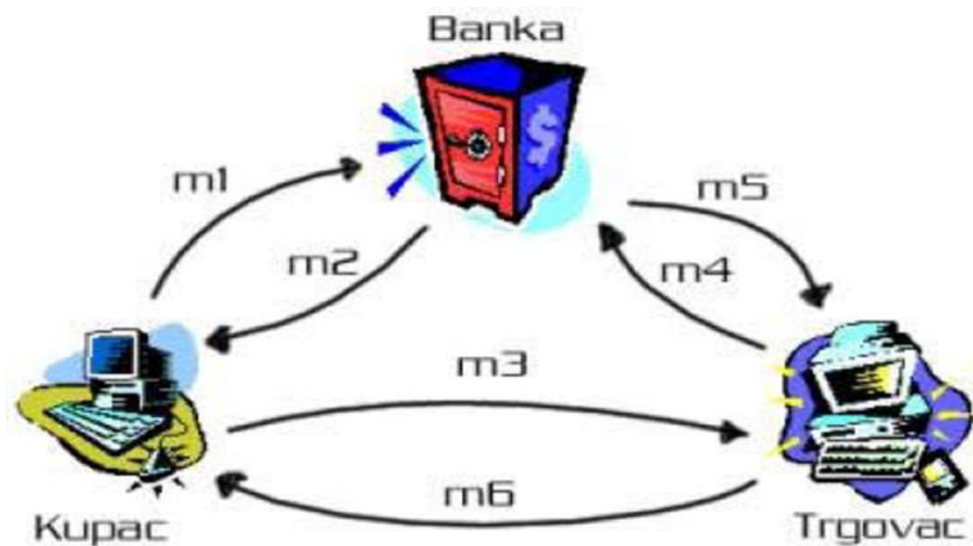
- **kupac** šalje elektronski **novac trgovcu** (**m3**);
- **trgovac** proverava **digitalni potpis** banke na primljenoj novčanici



Protokol bez anonimnosti

Polaganje novca u banku:

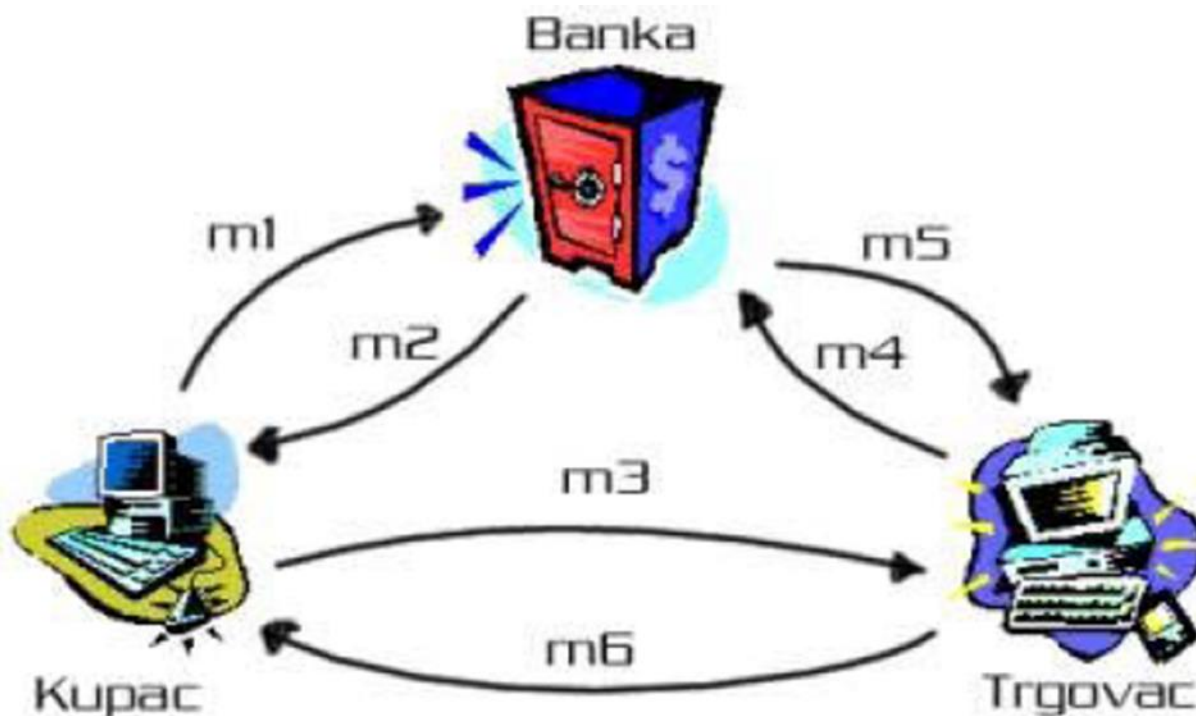
- **trgovac** šalje elektronsku **novčanicu banci** (**m4**);
- **banka** proverava **potpis** na novčanici;
- **banka** **upoređuje serijski broj** novčanice sa postojećima **u bazi upotrebljenih** elektronskih novčanica;
- **banka unosi serijski broj** novčanice **u bazu uporabljenih novčanica**;
- **banka uvećava račun trgovca**;



Protokol bez anonimnosti

Polaganje novca u banku:

- o **banka šalje** odgovor trgovcu (**m5**);
- o **trgovac šalje** kupljenu robu kupcu (**m6**)



● ● ● | Protokol bez anonimnosti

- U fazi podizanja novca iz banke, **banka stavlja digitalni potpis** na novčanicu i tako **onemogućava falsifikovanje** novčanica
 - Kada **banka proverava ispravnost** novčanice, ona **proverava digitalni potpis** i prema tome zaključuje da li je novčanica falsifikovana ili ne
- Kada **banka** oblikuje elektroničku novčanicu, **stvara i serijski broj novčanice** koji **čuva u svojoj bazi**
- Na taj se način **onemogućava višestruko korišćenje** iste novčanice

● ● ● | Protokol bez anonimnosti

- *Kod stvaranja elektronske novčanice* - banka može *zapamtiti vezu između kupca i serijskog broja novčanice* i time *ugroziti privatnost kupca* i pratiti njeno kretanje
 - Sistem *ne garantuje anonimnost* - postoji mogućnost praćenja transakcija
 - Dakle, *narušavanje privatnosti je nedostatak* ovog protokola
- Spomenuti nedostatak je ispravljen u *protokolu sa anonimnošću*

● ● ● | Protokol sa anonimnošću

- Protokol sa anonimnošću osigurava anonimnost kupca pred bankom
- *Banka nije u mogućnosti pratiti kretanje novčanice* kroz transakciju u sistemu plaćanja elektronskim novcem
- To se ostvaruje mehanizmom slepog potpisa sa *delomičnim uvidom* u sadržaj dokumenta
- Protokol bez anonimnosti se razlikuje od protokola sa anonimnošću u prvoj fazi, kada kupac podigne novac iz banke

● ● ● | Protokol sa anonimnošću

Podizanje novca iz banke:

○ **kupac oblikuje n** elektronskih novčanica koje nose

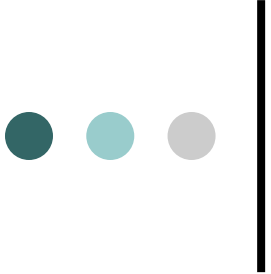
a) jednaki iznos,

b) različite serijske brojeve

c) (oblikovanu - heširanu) identifikacionu informaciju

● **Problem**: Sa anonimnošću kupca nastaje problem otkrivanja počinitelja prevare i zaštite prodavca

● **Mehanizam identifikacione informacije** otkriva identitet učesnika transakcije koji je pokušao ili izvršio **prevaru dvostruke potrošnje**, dok poštenog učesnika **ostavlja u anonimnosti**



Protokol sa anonimnošću

Podizanje novca iz banke:

identifikaciona informacija – proces oblikovanja

- Rezultat oblikovanja - ***n binarnih nizova*** dobijenih na bazi ***binarnog zapisa identifikacione informacije***
- Identifikaciona informacija se generiše na temelju ***podataka karakterističnih za osobu*** koja generiše elektronsku novčanicu
 - Ti podaci mogu biti ***ime i prezime osobe***, e-mail, telefonski broj i ostale bitne ***informacije*** o osobi ***koje ga identifikuju***

● ● ● | Protokol sa anonimnošću

Podizanje novca iz banke:

identifikaciona informacija – proces oblikovanja

- Dalja obrada....
- Tako generisani identifikacioni nizovi razdvajaju se ***postupkom deljenja na dva dela***
- Vrš se ***heširanje*** (formiranje otiska) svakog od n ***identifikacionih nizova*** i to ***svaki deo posebno***
- ***Dužina otiska*** svakog dela je (najčešće) ***1***
- Tako obrađeni identifikacioni nizovi se pridružuju (***postaju sastavni deo***) ***novčanice***

● ● ● | Protokol sa anonimnošću

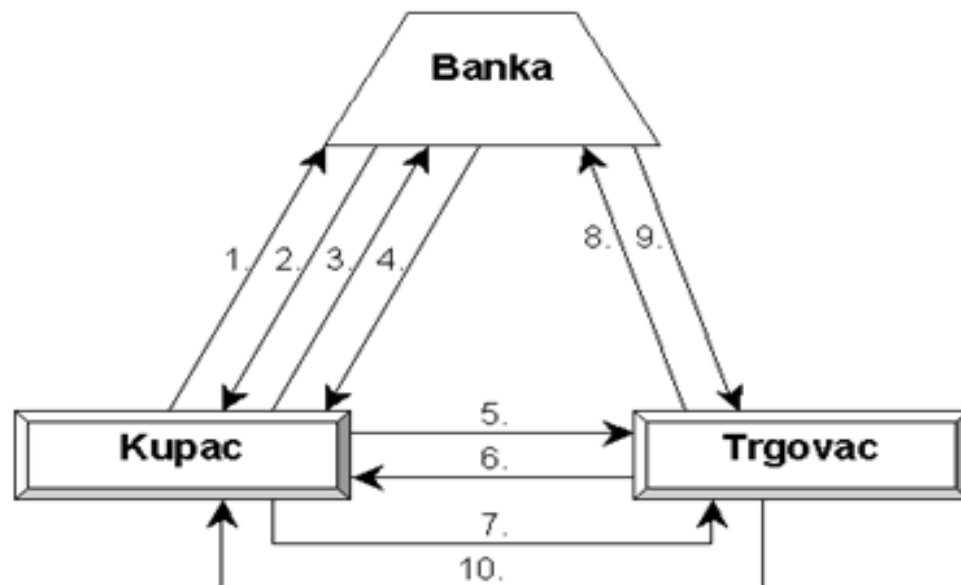
Podizanje novca iz banke:

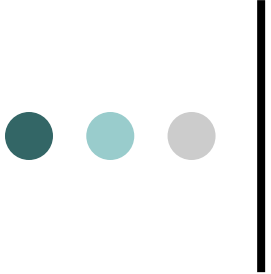
- **kupac** prikriva n elektronskih novčanica
- **kupac** šalje n prikrivenih elektronskih novčanica **banci** (korak 1.)
- **banka** šalje zahtev **kupcu** za otkrivanje $n-1$ slučajno odabrane elektronske novčanice (korak 2.)
- **kupac** šalje **banci** $n-1$ traženi **faktor slepoće** i $n-1$ odgovarajuću **identifikacionu informaciju** (korak 3.)
- **banka** proverava valjanost $n-1$ elektronske novčanice (iznos i identifikacionu informaciju)

Protokol sa anonimnošću

Podizanje novca iz banke:

- **banka potpisuje preostalu** elektronsku novčanicu
- **banka šalje** potpisanu elektronsku novčanicu **kupcu** i umanjuje račun kupca (**korak 4.**)
- **kupac uklanja faktor slepoće** sa potpisane novčanice i **proverava potpis banke**

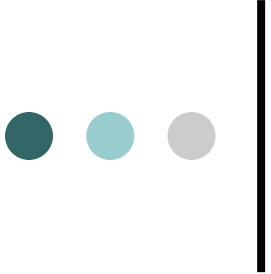




Protokol sa anonimnošću

Plaćanje:

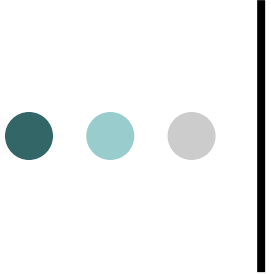
- **kupac** šalje potpisanu elektronsku **novčanicu trgovcu** (**korak 5.**)
- **trgovac** proverava digitalni potpis **banke** uz elektronsku novčanicu
- **trgovac** šalje **kupcu** slučajno generisani **odabirući niz** (**korak 6.**)
 - **Niz 0 i 1** (dužine n) pri čemu, **0 znači prvu**, dok **1 predstavlja drugu polovinu** identifikacionog niza
 - Redosled 0 i 1 u odabirućem nizu predstavlja redosled identifikacionih nizova **čije se polovine traže**



Protokol sa anonimnošću

Plaćanje:

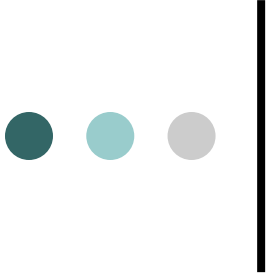
- **kupac** šalje tražene informacije **trgovcu** (**korak 7.**)
- **trgovac** *proverava valjanost dela identifikacione informacije* na elektronskoj novčanici
 - Nakon što kupac pošalje polovine identifikacionih nizova - **trgovac ih upoređuje** sa onima na elektronskoj novčanici
 - Treba napomenuti da se na elektronskoj novčanici nalaze **otisci polovina identifikacionih nizova**, tako da trgovac **pre upoređivanja** obavlja **hash funkciju** nad svakom primljenom polovinom



Protokol sa anonimnošću

Polaganje novca u banku:

- **trgovac šalje**
 - a) **potpisanu** elektronsku **novčanicu**,
 - b) **odabirajući niz**,
 - c) **deo (otkrivene) identifikacione informacije i**
 - d) **broj bankovnog računa** (korak 8.)
- banci**



Protokol sa anonimnošću

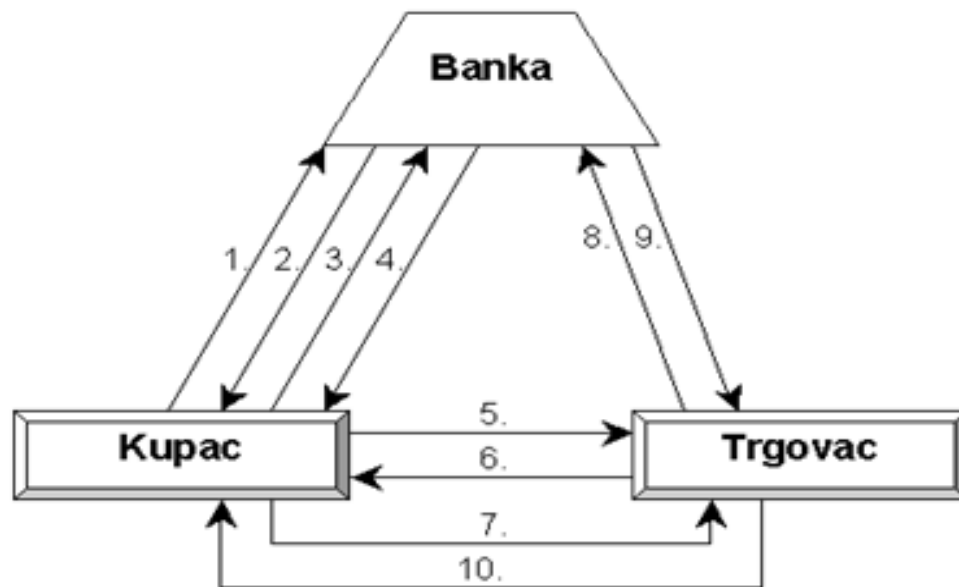
Polaganje novca u banku:

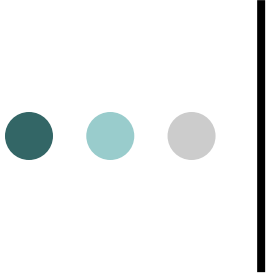
- **banka** *proverava digitalni potpis* uz primljenu elektronsku novčanicu
- **banka** *upoređuje serijski broj* elektronske novčanice sa onima *u bazi upotrebljenih novčanica*
- **banka** *unosí serijski broj* elektronske novčanice, *odabirući niz i deo (otkrivene) identifikacione informacije* u bazu upotrebljenih elektronskih novčanica

Protokol sa anonimnošću

Polaganje novca u banku:

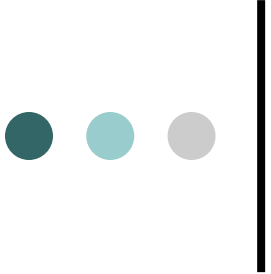
- **banka** šalje odgovor **trgovcu** o ispravnosti elektronske novčanice i uvećava račun trgovca (**korak 9.**)
- **trgovac** proverava odgovor **banke**
- **trgovac** šalje robu **kupcu** (**korak 10.**)





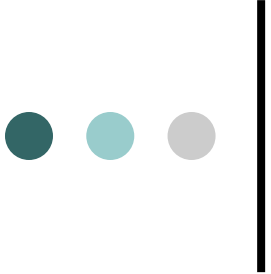
E- cash

- **E-cash** je **skup protokola** i **metoda** korišćenih za **obavljanje finansijskih transakcija mikroplaćanja preko** računarskih mreža poput **Interneta** (DigiCash – 1996. godine) **baziranom na tokenima**
- Podržava:
 - a. **Anonimnost**
 - b. **Nemogućnost praćenja**
 - c. **Sistem plaćanja baziran na tokenima koji koristi on-line verifikaciju**
 - d. ⁹²**Bi-direkcionalna plaćanja**



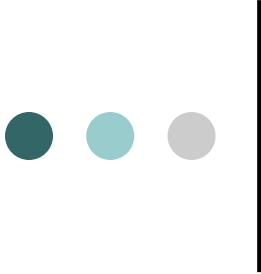
E- cash

- Protokol se temelji na korišćenju „**elektronskih kovanica**“ (**E-cash tokena**), odnosno **niza znakova** koji sadrži:
 - podatke o nominalnoj vrednosti,
 - serijski broj koga je pružila **banka** koja podržava e-cash tehnologiju i
 - digitalni potpis **banke**
- „**Elektronske kovanice**“ - osnovna jedinica plaćanja u transakcijama



E- cash

- U slučaju da ne postoji dovoljan broj manjih kovanica, ***kupac zahteva od banke*** da mu razmeni jednu veću ***na dve manje*** kovanice, od kojih ***jedna ima iznos isti kao račun*** koji treba podmiriti



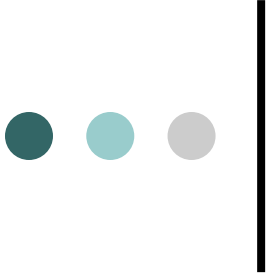
E- cash

- ***Nakon obavljanja plaćanja***, određeni broj digitalnih kovanica se **prenosi** preko Interneta, ***od kupca do trgovca***
- ***Krajnji rezultat*** - ***umanjivanje*** broja kovanica ***kupca*** za plaćeni iznos i ***uvećavanje*** broja kovanica ***trgovca***
- Kovanice se ***u svakom trenutku*** mogu ***staviti ili povući sa računa***, a sve transakcije se zapisuju kako bi se olakšala evidencija

E- cash

- ***Svaki korisnik E- cash sistema*** mora instalirati odgovarajući **wallet- softver** koji omogućuje
 - on-line pristup računu
 - manipulacije sa kovanicama

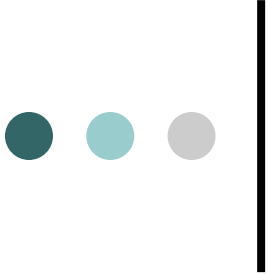




E- cash

Podizanje novca s bankovnog računa:

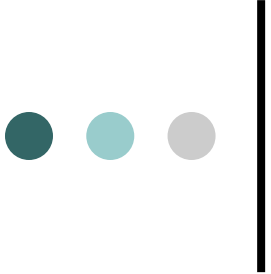
- **kupac stvara** slučajne **brojeve** za **serijske brojeve** e-cash kovanica
 - Serijski brojevi se prikrivaju (**slepi potpis**)
 - Takve kovanice se šalju e-cash banci
- **banka proverava** ispravnost i **tereti** bankovni **račun vlasnika**;
- **banka potvrđuje** (potpisuje) kovanice i vraća ih kupcu;
- **kupac uklanja faktor slepoće** s novčanica



E- cash

Plaćanje:

- **kupac šalje zahtev** za kupovinom **trgovcu**
- **trgovac šalje zahtev** natrag **kupcu** da upotrebom virtualnog novčanika **pošalje novac**
- **kupac potvrđuje transakciju** i upotrebom programskog paketa (**virtualnog novčanika**) **prebacuje** tačan broj kovanica

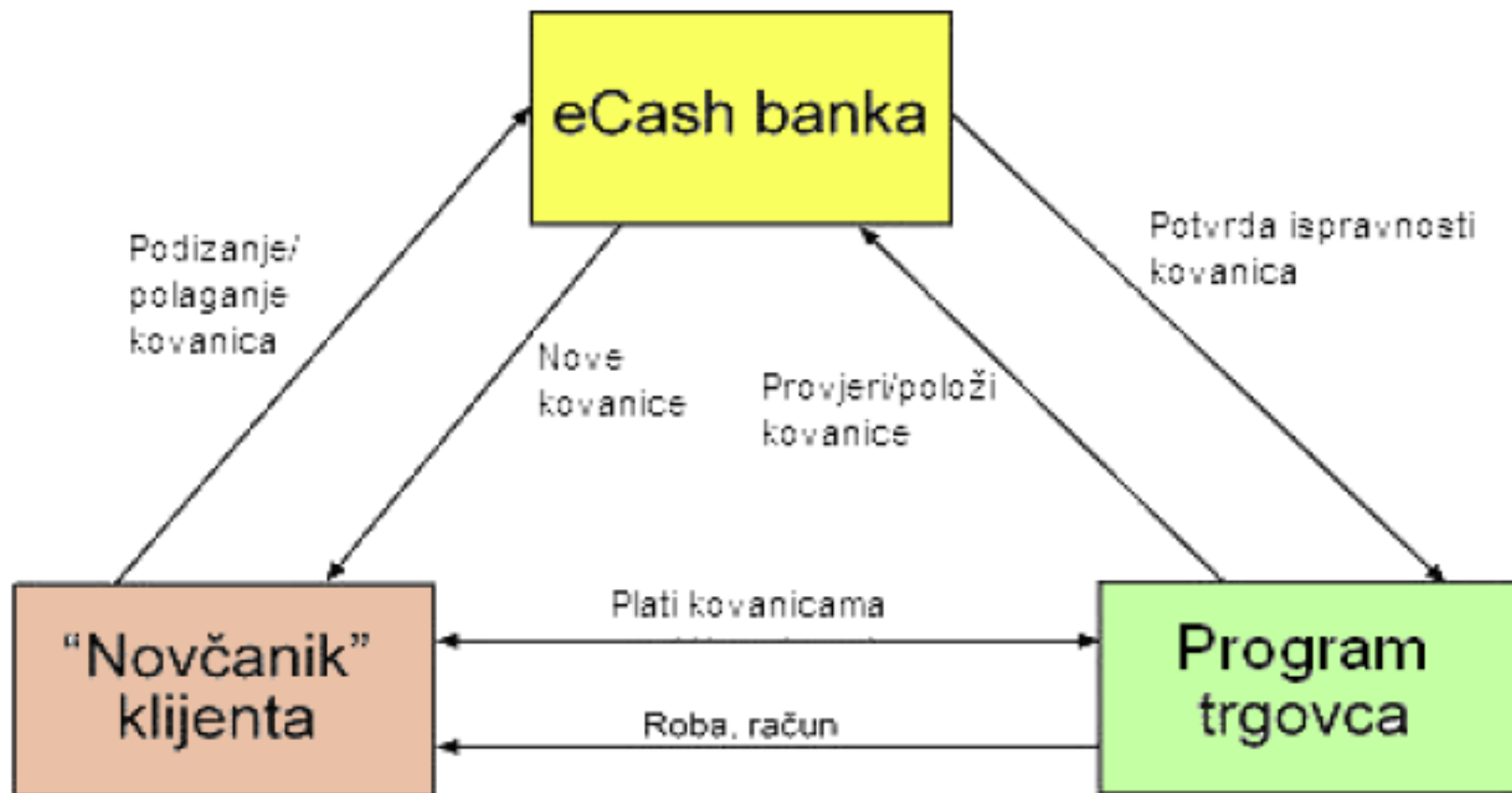


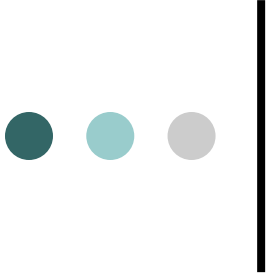
E- cash

Polaganje novca na račun:

- **trgovac** mora **proveriti ispravnost** kovanica i šalje ih **banci** koja ih je izdala da se uveri da novac već nije bio korišćen
- **banka proverava serijski broj** zbog višestruke uporabe
- Ako su **kovanice valjane**, **banka uništava kovanice**,
(**a**) **dodaje serijski broj u bazu** podataka potrošenih kovanica i (**b**) **povećava račun trgovca**

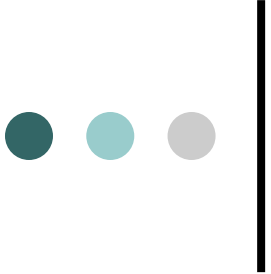
Model E- cash sistema





E- cash

- **Elektronske kovanice** koje se koriste u e-cash sistemu **jedinstvene su** po tome što ih **stvara kupac** pre nego ih potpiše banka
- Svaka **kovanica** ima **serijski broj** koji joj je **dodelio virtualni novčanik**
- **Serijski brojevi** su **izabrani slučajno** i **dovoljno su veliki** – malo je verovatno da će bilo ko drugi ikada stvoriti isti serijski broj
- **Serijski broj** se **potpisuje slepim potpisom**



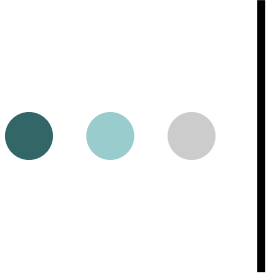
E- cash

- ***Potpis na kovanici*** sa kojeg je ***uklonjen faktor slepoće*** je ***kao i svi drugi normalni digitalni potpisi***
- ***Ne postoji način*** na koji bi se moglo ***prepoznati*** da je kovanica ***potpisana upotrebom slepog potpisa***

● ● ● | Mondex

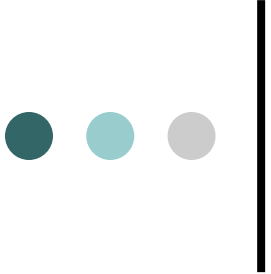
- Mondex **sistem digitalnog (elektronskog) novca**
- Razvila ga je firma **Mondex U.K.**
- **MasterCard** kupovinom kontrolnog paketa postaje njen **vlasnik**
- Mondex je **razvijen kao off-line sistem**, ali je kasnije **prilagođen Internetu**





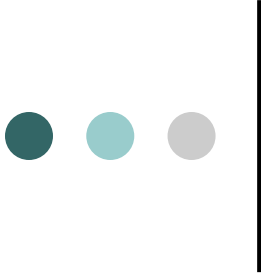
Mondex

- **Zasnovan na karticama sa mikročipom**, a **jedinstven** je po tome što **omogućava transfer sa kartice na karticu**
- Svaka kartica ima **jedinstven ID** – na osnovu koga je **jednostavno otkriti identitet korisnika**
- **Mondex- novac** se smešta na **korisnikovu karticu**



Mondex

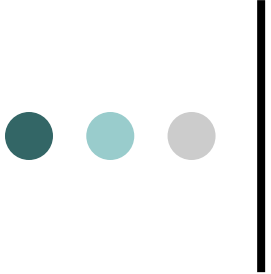
- Mondex novac se **može prenositi sa jedne kartice na drugu** neograničen broj puta, bez potrebe **verifikacije od strane neke banke**
- Najpribližniji je realnom novcu
- Ključna razlika izmenu Mondex-a i realnog novca je **mogućnost praćenja transakcija**, koju pruža Mondex
 - Mondex kartice **evidentiraju svaku transakciju** putem **jedinstvenog identifikatora (ID)**, koji se može koristiti za praćenje transakcija, ako je potrebno



Mondex

Procedura plaćanja je vrlo jednostavna

- ***Korisnici preuzimaju digitalni keš iz banke***
(uključena u Mondex sistem)
- Kada želi da ***naruči robu ili usluge od trgovca*** u čiji je sajt uključena Mondex opcija – ***korisnik ubacuje karticu u čitač*** kartice i ***obavlja transfer*** do trgovca
- **Prednost Mondex-a** – **ista kartica** se može koristiti i ***on-line*** i za ***plaćanja u realnom svetu***



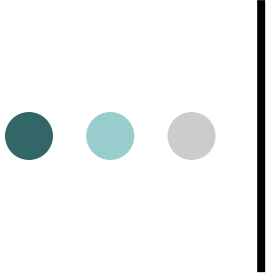
Mondex

- Nedostatak Mondex-a – *kupac mora da poseduje čitač kartice* koji ugrađuje u svoj PC
- *E-cash* je *zasnovan samo na softveru*
- Brojne kompanije (*VeriFone, GemPlus,...*) koje *proizvode čitače i smanjuju im cenu – uklonjena je ova barijera*

Mondex

- ***Ključni momenat*** kod Mondex-a je **bezbednost**
- Postoji u ***dva primarna aspekta*** sistema:
 - U hardveru ***na kartici***
 - U procesu ***prenosa vrednosti***

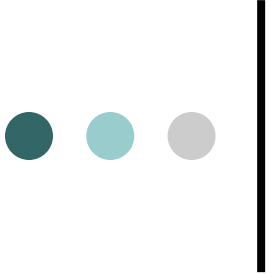




Mondex

Sušтина hardverske bezbednosti

- Mondex-ov digitalni ***novac ne može postojati nigde osim na Mondex kartici***
- ***Obezbeđena je potpuna sigurnost*** jer ***ni jedna druga kartica*** sa čipom ili hardverski uređaj – ***ne može da komunicira*** sa pravom Mondex karticom
- ***Svaka kartica*** ima ***Mondex digitalni potpis***



Mondex

Proces transfera je krajnje bezbedan

- *Transfer novca* između dve kartice *podrazumeva proveru autentičnosti*
- Transfer između kartica *se obavlja u sekvenama*, tako da novac ne može istovremeno postojati na dva mesta
- Novac se prvo skida sa kartice pa se tek onda upisuje u drugu karticu

● ● ● | Mondex - Problemi

- Značajan nedostatak ovog sistema - **transakcije nisu u potpunosti anonimne**
- Mondex karticu **nije moguće naručiti bez otkrivanja identiteta** (za razliku od pre-paid telefonske kartice)
 - Svaka kartica ima **jedinstven ID** – na osnovu koga je **jednostavno otkriti identitet korisnika**
- **Gubitak Mondex kartice** je isto što i **gubitak novčanika punog para** (za razliku od platnih kartica)

● ● ● | Mondex - Problemi

- Mnogo **značajnija barijera** je – ekonomske prirode
- Bankama nije jasno **kako će profitirati** na njemu
- Ako Mondex- novac **funkcioniše nezavisno od banke**

GDE JE TU REZON BANKE DA TO RADI?

- Novac se kupuje od Mondexa
- Banke ga prosleđuju korisnicima
- Banke ne zarađuju na proviziji obrade transakcija – sistem ne zahteva nužno prisustvo banaka
- Banka učestvuje jedino ako korisnik diže keš

● ● ● | Mondex - Bezbednost

- Aktivan i skriven **“security software”**
 - Security- metod konstantno **se menja**
 - ITSEC E6 nivo (vojni)
- VTP (*Value Transfer Protocol*)
 - **Globalno** jedinstven broj kartice
 - **Globalno** jedinstven broj transakcije
 - Korisnička identifikacija je na osnovu upita i odgovora
 - **Digitalni potpis**
- **MULTOS operativni sistem**
 - ¹¹³**firewall** je na “chip-u”