SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINARSKI RAD
IZ KOLEGIJA
SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

ELEKTRONIČKI NOVAC

STUDENT: **Mirko Poljak**
JMBAG: **0036399061**
SMJER: **Industrijska elektronika**

Zagreb, 2006.

Sadržaj

1. Vrste elektroničkog plaćanja

Klasične, neelektroničke, vrste plaćanja mogu se podijeliti na dvije grupe: notacijsko ili negotovinsko i simboličko ili gotovinsko. Vrste elektroničkog plaćanja su ekvivalent nekog od klasičnih načina plaćanja.
Razlika između ove dvije vrste plaćanja je u načinu na koji novac mijenja vlasnika. Notacijski ili negotovinski način temelji se na dokumentu, npr. nalogu, čeku ili kartici, koji sam nema novčanu vrijednost. Ovakav je dokument svojevrsni nalog banci u kojoj je novac pohranjen da ga u trenutku kada joj se prezentira ovakav dokument prebaci s računa kupca na račun trgovca. Simbolički ili gotovinski sustav temelji se na simbolu koji ima stvarnu vrijednost, npr. novčanica ili kovanica. Samim ustupanjem simbola ustupa se i novčana vrijednost.

1.1. Negotovinski sustavi

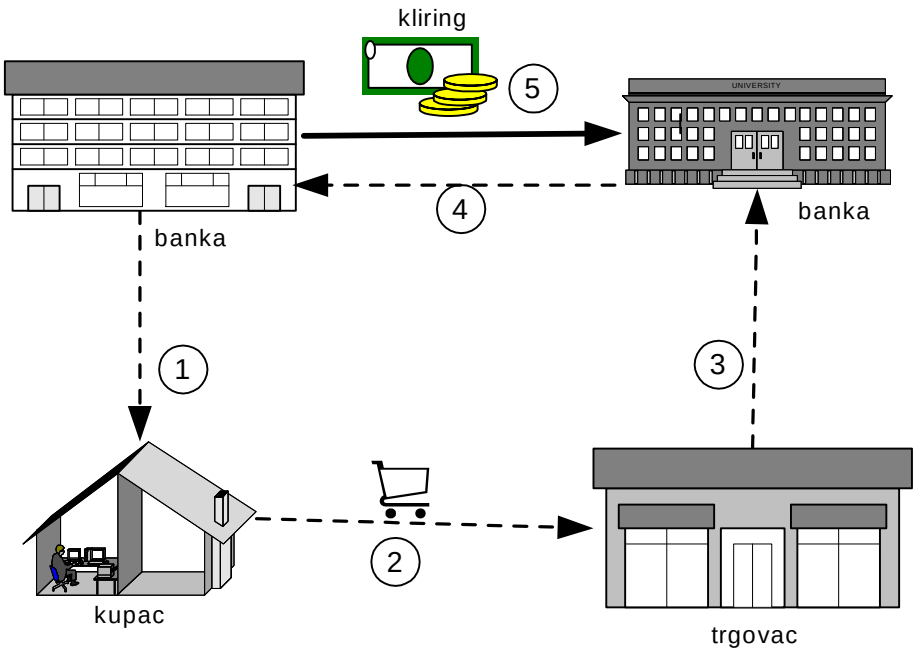
Kod negotovinskog načina plaćanja kupac koji ima otvoren račun u banci koristeći jedan od oblika bezgotovinskog plaćanja trgovcu predaje elektronički nalog za prebacivanje sa svog računa na račun trgovca. Dokument preko kojeg se daje nalog može biti e-ček, kreditna kartica, debitna kartica itd.

1.1.1. E-ček

Elektronički ček je elektronički ekvivalent klasičnog papirnatog čeka. Kupac ga izdaje trgovcu, a trgovac ga polaže u svoju banku koja obavlja naplatu od banke izdavatelja e-čeka. Proces naplate teče na sljedeći način:

1. Banka kupcu izdaje e-ček potpisan digitalnim potpisom banke.
2. Kupac upisuje u e-ček iznos i datum, potpisuje ga svojim digitalnim potpisom i predaje trgovcu. Trgovac izdaje robu kupcu.
3. Trgovac upisuje na ček svoj broj računa i prosljeđuje e-ček svojoj banci, potpisujući ga svojim digitalnim potpisom.
4. Trgovčeva banka provjerava potpis trgovca i potpis banke izdavatelja i prosljeđuje ček banci izdavatelju na naplatu.
5. Banka izdavatelj provjerava svoj digitalni potpis i digitalni potpis kupca na prispjelom čeku, provjerava stanje novca na računu i prebacuje novac s računa kupca na račun trgovca (ako je sve u redu).

E-ček predstavlja rizik za trgovca. Razlog je tome što prodavač ne može znati ima li kupac na svom računu u banci dovoljno novca za pokriće čeka. Osim toga, kupac može falsificirati digitalni potpis. Ako želi biti siguran, trgovac mora imati on-line vezu s bankom izdavateljem čeka što bitno komplicira i poskupljuje transakciju jer banaka može biti mnogo.

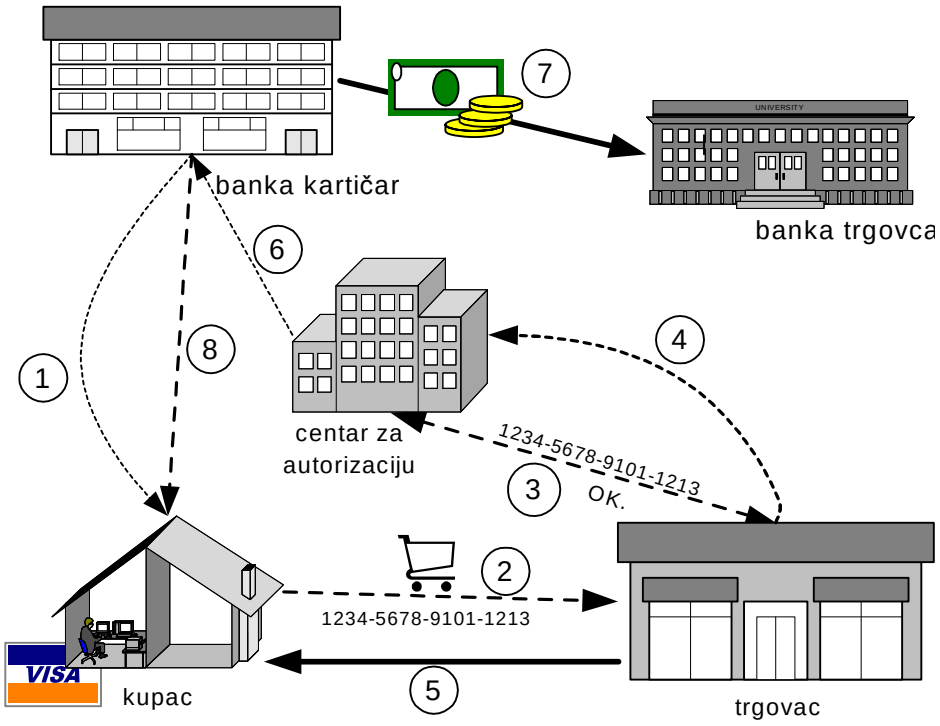


Slika 4.1. Dijagram transakcije u slučaju plaćanja e-čekom

1.1.2. Kreditna kartica

Plaćanje kreditnom karticom je klasični, neelektronički, način plaćanja. Kako se kreditnom karticom plaća prijenosom informacije, moguće je njome plaćati u sustavima koji omogućavaju elektronički prijenos poruke. Plaćanje kreditnom karticom zbog velike je raširenosti kartica postalo najzastupljeniji način plaćanja na Internetu. Proces plaćanja kreditnom karticom teče na sljedeći način:

1. Banka izdaje kupcu kreditnu karticu.
2. Kupac šalje trgovcu podatke sa svoje kartice (broj kartice, ime nositelja, datum isteka valjanosti).
3. Trgovac preko on-line sustava provjerava valjanost kartice kod banke izdavatelja ili neke druge autorizacijske institucije.
4. Ako je kartica valjana, trgovac šalje autorizacijskoj instituciji iznos koji kupac želi platiti. Ako se iznos može naplatiti, dobiva odobrenje za naplatu.
5. Nakon što je dobio odobrenje, bilježi kod sebe broj transakcije koji je dobio skupa s odobrenjem. Trgovac predaje kupcu robu.
6. Banka kupca obavlja transakciju s bankom trgovca (kliring).
7. Kartičar periodično plaća trgovcu za sve uspješno autorizirane transakcije.
8. Kupac periodično dobije račun od kartičara za sve troškove koje je napravio u tijeku mjeseca.



Slika 4.3. Dijagram transakcije u slučaju plaćanja kreditnom karticom

Plaćanje kreditnom karticom preko Interneta ima nekoliko nedostataka:

- Sigurnost transakcije – ako se treća strana (lopov) dokopa broja kartice može neovlašteno trošiti raspoloživi novac.
- Cijena transakcije – postupak autorizacije i naplate košta negdje oko 20 centi plus 3–5% od vrijednosti transakcije, tako da nije isplativ u slučajevima malih iznosa.
- U trenutku naplate trgovac mora imati on-line vezu s bankom, kako bi provjerio valjanost kartice.
- Transakcija je moguća samo između kupca i trgovca, nije moguća između dviju fizičkih osoba.
- Banka - izdavatelj kartice - raspolaže svim podacima o iznosima, mjestima i vremenima plaćanja pa skladištenjem tih podataka može pratiti klijentove potrošačke navike, narušavajući tako njegovu privatnost.

1.1.3. Debitna kartica

Debitna kartica je vrlo slična kreditnoj kartici. Razlika je u tome da kupac mora u trenutku kupnje imati novac na računu. Trgovac preko on-line veze s bankom istodobno provjerava valjanost kartice i odmah prebacuje novac s računa kupca na svoj račun. Debitne kartice obično su zaštićene 4-znamenkastim brojem (engl. *personal identification number*, kratica PIN), tako da je u slučaju krađe lopov ne može neovlašteno koristiti. Četveroznamenkasti PIN dovoljan je sigurnosni element u slučaju kada ga se mora osobno ukucavati na tipkovnici bankomata, no u slučaju kada se on predaje elektronički nije dovoljan. Način plaćanja debitnom karticom ne omogućava naknadno prekidanje uplate, kao što je to moguće kod kreditnih kartica.

Debitna kartica ne predstavlja rizik za trgovca, no zahtijeva da se cijeli proces provjere i prijenosa novca obavi prije isporuke robe kupcu. Uz već spomenuti rizik kupca, ovo debitnu karticu čini nepraktičnom za korištenje preko Interneta.

1.2. Gotovinski sustavi

Za razliku od negotovinskog sustava gdje novac zapravo nikada ne napušta banku ili banke, u gotovinskom sustavu sama reprezentacija novca nosi njegovu vrijednost. Ovo znači da se iznos na računu umanjuje čim se e-novčanica podigne iz banke. U slučaju da se e-novčanica izgubi, vlasnik bez nje ostaje trajno. Ova vrsta e-novca analogna je klasičnoj gotovini i zato se obično naziva e-gotovina.

1.2.1. E-gotovina

E-gotovina ima karakteristike slične "materijalnoj" gotovini. "Materijalne" gotovina je univerzalno prihvaćena, prihvaćena je za plaćanja pravnih i fizičkih osoba, kupac pri uporabi ostaje anoniman, verifikacija autentičnosti novčanice lako se obavlja pri samoj kupnji, nije potreban račun u banci, prenosiva je između fizičkih i pravnih osoba, korisnici ne moraju biti poslovno sposobni (npr. punoljetni).
Osim navedenih dobrih strana, gotovina ima i važne nedostatke: relativno visoki troškovi vezani uz proizvodnju i distribuciju, nepraktičnost fizičkog nošenja veće količine, nepogodnost za mala plaćanja (mikroplaćanja, manja od 1 USD), na raspolaganju je ograničen broj nominacija, neupotrebljivost u području digitalne ekonomije, lako ga je ukrasti, može se krivotvoriti, postoji više valuta, a konverziju prate troškovi.
E-gotovina mora zadržati dobre strane, a eliminirati što je više moguće loših osobina klasične gotovine. Idealna e-gotovina mora zadovoljiti sljedeće zahtjeve:

- mora biti omogućeno jednostavno pretvaranje prave gotovine odnosno nekog drugog oblika novčane vrijednosti u e-gotovinu i obrnuto
- mora se onemogućiti krivotvorenje e-novčanice
- mora se onemogućiti plaćanje dva puta istom e-novčanicom
- mora se sačuvati anonimnost kupca
- mora biti omogućena off-line provjera autentičnosti
- mora biti moguć prijenos bez dozvole treće strane (npr. banke)
- mora biti upotrebljiv bez računa u banci
- mora se omogućiti usitnjavanje u željene iznose
- mora biti neinteraktivan
- mora biti jednostavan i nezahtjevan za računalne resurse

Postoji nekoliko modela e-gotovine. Najčešće spominjani su Chaumov i Brandsov model. Oba ova modela ispunjavaju prva četiri zahtjeva. Chaumov model predviđa detekciju dvostruke potrošnje, a Brandsov njezino sprječavanje hardverskim sklopom. Samo Brandsov model omogućava i usitnjavanje. Ni jedan ni drugi model ne predviđaju mogućnost prijenosa između osoba bez posrednika (banke).

Kod prijenosa e-gotovine između dva sudionika javljaju se dva problema:

- pri svakom prijenosu e-novčanica "raste", pošto se na nju dodaju podaci o novom vlasniku

- s obzirom na to da se polaganje novca u banku odlaže na neodređeno dugo vrijeme, odgađa se i potencijalna detekcija višestruko potrošene novčanice.

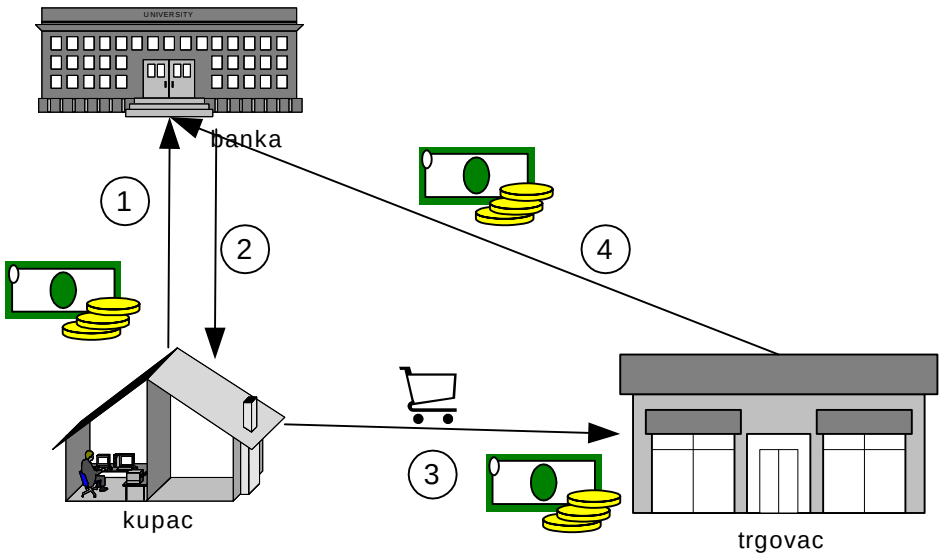
Očito, sustav koji će omogućavati prenosivost mora počivati na fizičkom sprječavanju dvostruke potrošnje, pošto sama detekcija nije dovoljna.
Neinteraktivnost podrazumijeva da je moguće poslati e-gotovinu samo posredstvom jedne jedine poruke, bez dodatne interakcije među korisnicima. Ovo je u potpunosti različito od ranije predloženih načina elektroničkog plaćanja koji predviđaju iterativni postupak između kupca i banke pri podizanju novca, i/ili između kupca i trgovca prilikom plaćanja.

1.2.2. Plaćanje e-gotovinom

E-gotovina se sastoji od e-novčanica koje su ekvivalenti papirnatih novčanica i kovanica. Prije nego što može raspolagati s e-gotovinom, kupac je mora podignuti u banci. Prilikom plaćanja trgovcu mora biti omogućena provjera autentičnosti novčanice. Postoje dva modela, ovisno o tome ima li trgovac on-line vezu s bankom u trenutku plaćanja ili ne.

On-line

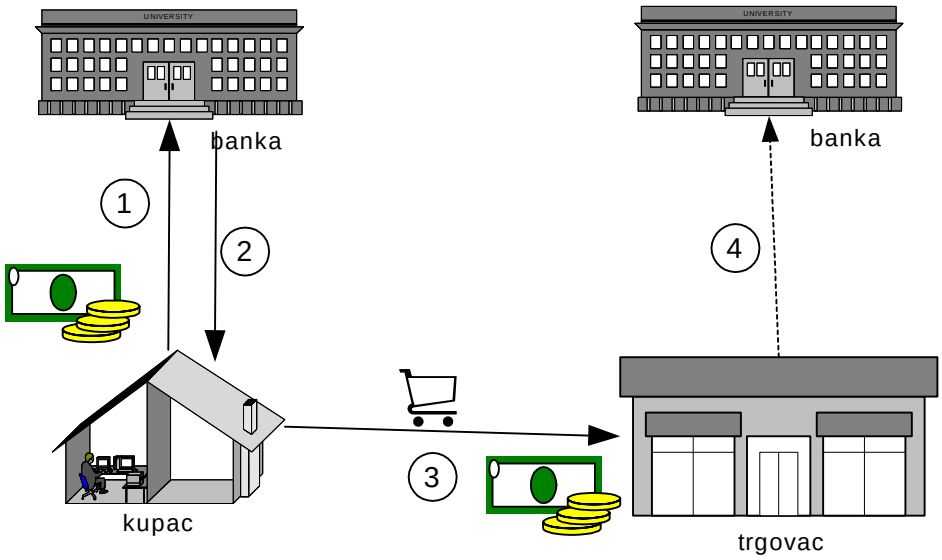
Ako trgovac ima on-line vezu s bankom u trenutku kupnje, tada promet e-gotovine teče na sljedeći način. Kupac podnese banci nalog za izdavanje e-novčanice. Banka zaprima zahtjev i provjerava identitet podnositelja zahtjeva. Ako je provjera uspješna, banka umanjuje saldo na računu podnositelja zahtjeva i izdaje e-novčanicu u zahtijevanom iznosu, s jedinstvenim serijskim brojem i digitalnim potpisom banke s bančinim privatnim ključem. U bazu podataka bilježi se serijski broj novčanice. Kupac odlazi u virtualnu trgovinu gdje kupuje robu ili usluge od trgovca te mu predaje elektroničku novčanicu. Trgovac kontaktira banku i traži provjeru ispravnosti dobivene novčanice. Ako je novčanica ispravna, trgovac je odmah polaže na svoj račun i kupcu daje robu.



Slika 4.5. Promet e-gotovine u on-line sustavu

Off-line

U off-line sustavu trgovac nema vezu s bankom u trenutku plaćanja, pa stoga mora imati način provjere autentičnosti e-novčanice na licu mjesta. Način plaćanja u off-line sustavu teče na sljedeći način. Kupac podnese banci nalog za izdavanje e-novčanice. Banka zaprima zahtjev, provjerava identitet podnositelja zahtjeva i ako je provjera uspješna, umanjuje se saldo na računu podnositelja zahtjeva te izdaje e-novčanicu u zahtijevanom iznosu s jedinstvenim serijskim brojem i digitalnim potpisom banke s bančinim privatnim ključem. U bazu podataka zabilježi se serijski broj novčanice. Kupac posjećuje virtualnu trgovinu gdje kupuje robu ili usluge od trgovca, te predaje trgovcu e-novčanicu. Trgovac provjerava ispravnost bančinog potpisa uz pomoć bančinog javnog ključa. Trgovac izdaje robu kupcu i zatim polaže novac u banku. Banka provjerava autentičnost potpisa izdavatelja i provjerava je li novčanica već ranije položena. Ako je sve u redu, uvećava se iznos na računu trgovca.



Slika 4.6. Promet e-gotovine u off-line sustavu

2. Problemi u plaćanju elektroničkim novcem

U prethodnom je poglavlju predstavljen način plaćanja e-gotovinom. Predstavljeni model je jednostavan i ima mnoge nedostatke. S obzirom na to da banka u trenutku izdavanja novčanica kupcu zna njegov identitet, može za svaku izdanu novčanicu uz serijski broj u bazi podataka zabilježiti datum i vrijeme, te identitet kupca. Nakon što trgovac položi novac u banku, banka može točno znati kada, gdje i za koji iznos je kupac nešto kupio, što znatno narušava privatnost kupca. S obzirom na to da su e-novčanice samo podaci (na disku ili u memoriji na kartici), kupac bi mogao pojedinu novčanicu jednostavno kopirati i njome platiti dva puta u dvije različite trgovine. Tada bi onaj trgovac koji je kao drugi pokušao položiti novac naišao na odbijanje banke da mu prizna tu novčanicu. Isto tako bi trgovac mogao novčanicu umnožiti prije polaganja u banku, i položiti je više puta. Ovaj problem zove se problem dvostruke potrošnje i ključan je u razmatranju modela e-gotovine.
Kako bi se moglo provjeriti je li novčanica već ranije položena u banku, trgovac mora položiti gotovinu u istu onu banku koja ju je izdala, u banku koja sa bankom izdavateljem ima on-line vezu ili negdje mora postojati centralni registar svih novčanica u optjecaju.

2.1. Anonimnost kupca

Kako bi se banci onemogućilo stvaranje baze podataka s identitetom i serijskim brojem novčanice, može se prepustiti kupcu da generira serijski broj novčanice, koji će zatim tehnikom prikrivanja sakriti od pogleda banke, te će takvu novčanicu predati banci na slijepi potpis. S obzirom na to da banka potpisuje novčanicu čiji joj je sadržaj nepoznat, primjenjuje se tehnika "podijeli i odaberi" (engl. *cut and choose*). U modelu koju je predložio D. Chaum, kupac priredi *n* novčanica s istim iznosom, ali svaka od njih nosi drugi serijski broj. Svih *n* novčanica podnese banci na potpis, a banka odabere *n-1* i za njih od kupca zahtijeva da ih "otkrije". Ako pregled pokaže da je svih *n-1* novčanica stvarno na iznos koji je kupac rekao, i ako su serijski brojevi na njima ispravni, banka tada "na slijepo" potpisuje onu jednu preostalu novčanicu. Na ovaj način je onemogućeno kupcu da prevari banku, pošto ne može znati kojih *n-1* novčanica će banka pregledati. Tehnikom slijepog potpisa kupcu je garantirana anonimnost, a novčanica koju je dobio nosi ispravan potpis bankovnim tajnim ključem. Za veliko osiguranje protiv prevare kupca banka mora zahtijevati velik broj novčanica *n*, što za posljedicu ima opsežnu komunikaciju s kupcem.
S. Brands je predložio korištenje restriktivnog slijepog potpisa. Restriktivni slijepi potpis omogućava potpisniku da ograniči sadržaj koji potpisuje, a da taj sadržaj ne vidi. Kupac je na taj način "prikrio" svoj identitet, a da nije kompromitirao sadržaj novčanice. Usto, Brandsov sustav omogućava proizvoljne vrijednosti novčanice, čija se vrijednost smanjuje pri svakom plaćanju. Ove dvije osobine Brandsov model e-gotovine čine boljim rješenjem.

2.2. Problem dvostruke potrošnje

Problem dvostruke potrošnje može se riješiti na dva načina:

- prevencijom dvostruke potrošnje
- detekcijom dvostruke potrošnje

2.2.1. Prevencija dvostruke potrošnje

Prevenciju dvostruke potrošnje moguće je izvesti ako se elektronički novac nalazi pod nadzorom promatrača - softvera ili hardvera u koje izdavatelj e-novca (banka) ima povjerenja. Ovo je praktično izvedivo ako se koristi hardverska izvedba elektroničkog novčanika, u kojemu je kao poseban modul implementiran promatrač koji instalira banka i koji vodi brigu o tome da se jedna te ista novčanica nikada ne može izdati dva puta. Problem kod ovakvog promatrača je taj što kupac u njega ne može imati povjerenja. Može slutiti da promatrač o njemu i njegovim potrošačkim navikama skuplja podatke koje može proslijediti banci.

2.2.2. Detekcija dvostruke potrošnje

Ako ne postoji promatrač, ne postoji ni mogućnost sprječavanja dvostruke potrošnje. Ono što se može učiniti je otkriti slučaj kada se to dogodi kao i identitet krivca. Pretpostavimo da je identitet svakog kupca sadržan u samoj e-novčanici, ali tako da su za njegovo otkrivanje potrebna barem dva različita ključa, od velikog broja mogućih. Prilikom svake kupnje trgovac će od kupca zatražiti da mu generira jedan od ključeva, koji će zabilježiti na novčanicu. Kada trgovac položi novčanicu u banku, banka će imati ovaj ključ, ali kako samo jedan nije dovoljan, ne može otkriti identitet kupca. Ako kupac pokuša istu novčanicu potrošiti na drugom mjestu, drugi trgovac opet će zatražiti ključ te će ga upisati u novčanicu. Kada i druga novčanica dospije u banku, banka će usporedbom serijskih brojeva ustanoviti da je jedna te ista novčanica potrošena dva puta i imat će za nju dva ključa. Ako su ova dva ključa jednaka, to znači da je trgovac pokušao prevariti banku položivši dva puta jednu te istu novčanicu, a ako su različiti, znači da je kupac dva puta potrošio istu novčanicu i na osnovu njih će banka otkriti identitet kupca i prema njemu poduzeti sankcije.

3. Protokoli plaćanja elektroničkim novcem

3.1. Autentifikacijski SSL protokol

Glavna primjena SSL (Secure Sockets Layer) protokola je zaštita komunikacija preko Interneta gdje osigurava privatnost, autentičnost i integritet poruka koje se prenose između dvije strane. SSL se koristi pri prijenosu osjetljivih informacija (e-mail poruke, privatne informacije), ali i za obavljanje sigurnih transakcija preko Interneta (prijenos brojeva kreditnih kartica, elektroničkog novca). Protokol mora biti podržan na obje strane u komunikaciji - npr. pretraživač (browser) i poslužitelj (server) podržavaju SSL protokol i posjeduju svoje certifikate. Certifikat je skupina bitnih informacija koje identificiraju pretraživača (ili korisnika) i poslužitelja. Privatnost (tajnost) poruka koje izmjenjuju dvije strane u komunikaciji SSL protokolom osigurava se kriptiranjem. Autentičnost i integritet poruka SSL protokol osigurava korištenjem digitalnog potpisa uz svaku poruku koja se izmjeni u komunikaciji.
Prednost SSL protokola je što nije vezan za određeni informacijski servis (npr. WWW), već se koristi kao dodatak između pouzdanog prijenosnog sloja (TCP) i aplikacijskog sloja (HTTP, FTP, ...).

3.2. Protokoli plaćanja elektroničkim novcem

U opisanim protokolima plaćanja elektroničkim novcem sudjeluju tri strane: kupac, trgovac i banka. Sustavi kojima se obavlja plaćanje elektroničkim novcem neka su, zbog jednostavnosti, on-line sustavi kod kojih se provjera valjanosti elektroničke novčanice u banci može obaviti odmah po primitku novčanice. Svaki od protokola može se podijeliti u tri faze:

1. podizanje novca iz banke (engl. *withdrawal*)
2. plaćanje (engl. *payment*)
3. polaganje novca u banku (engl. *deposit*)

Ranije su opisani problemi anonimnosti kupca pri transakcijama s e-gotovinom. Protokoli plaćanja e-gotovinom mogu se, s tog gledišta, podijeliti u dvije skupine: protokol s anonimnošću i protokol bez anonimnosti kupca čiji opis slijedi.

3.2.1. Protokol bez anonimnosti

1. podizanje novca iz banke:
   - kupac šalje zahtjev banci za određenom količinom elektroničkog novca
   - banka oblikuje elektroničku novčanicu (sa serijskim brojem) te stavlja digitalni potpis
   - banka šalje elektroničku novčanicu kupcu te umanjuje njegov račun
2. plaćanje:
   - kupac šalje elektronički novac trgovcu
   - trgovac provjerava digitalni potpis banke na primljenoj novčanici

3. polaganje novca u banku:
- trgovac šalje elektroničku novčanicu banci
- banka provjerava potpis na novčanici
- banka uspoređuje serijski broj novčanice s postojećima u bazi uporabljenih elektroničkih novčanica
- banka unosi serijski broj novčanice u bazu uporabljenih novčanica
- banka uvećava račun trgovca
- banka šalje odgovor trgovcu
- trgovac šalje kupljenu robu kupcu

U drugoj točki podizanja novca iz banke, banka stavlja digitalni potpis na elektroničku novčanicu čime se onemogućava krivotvorenje novčanica. Pri stvaranju elektroničke novčanice generira se i serijski broj novčanice pomoću kojeg se onemogućava višestruko korištenje iste novčanice, odnosno njeno umnožavanje. Banka zapisuje serijski broj kod primitka novčanice te svako njeno sljedeće pojavljivanje s istim serijskim brojem označava je kao nevažeću. Banka može zapamtiti vezu između kupca i serijskog broja novčanice i time ugroziti privatnost kupca i pratiti njeno kretanje. Taj nedostatak je ispravljen u protokolu s anonimnošću.

3.2.2. Protokol s anonimnošću

Ovaj protokol, za razliku od prije opisanog, osigurava anonimnost kupca i onemogućava banku da prati kretanje e-novčanice u sustavu plaćanja e-novcem. Ta karakteristika se ostvaruje mehanizmom slijepog potpisa s djelomičnim uvidom u sadržaj e-novčanice. Jedina razlika ovog protokola i protokola bez anonimnosti je prva faza u kojoj se vrši podizanje novca iz banke:

1. podizanje novca iz banke:
- kupac oblikuje *n* e-novčanica koje nose jednaki iznos, ali različiti serijski broj
- kupac prikriva *n* e-novčanica
- kupac šalje *n* prikrivenih e-novčanica banci na digitalni potpis
- banka šalje zahtjev kupcu za otkrivanje *n-1* slučajno odabrane e-novčanice
- kupac otkriva banci *n-1* e-novčanicu
- banka provjerava valjanost *n-1* e-novčanice
- banka potpisuje neotkrivenu e-novčanicu
- banka šalje potpisanu e-novčanicu kupcu te umanjuje račun kupca
- kupac provjerava potpis banke

Druga i treća faza ovog protokola identične su drugoj i trećoj fazi protokola bez anonimnosti. Osiguranje anonimnosti dolazi od toga da kupac sam kreira elektroničku novčanicu sa serijskim brojem te je banka prikrivenu potpisuje što znači da nije u mogućnosti pročitati taj serijski broj i kasnije dovesti u vezu novčanicu i kupca. Međutim, i ovaj protokol ima nedostatak - nije moguće identificirati osobu koja je pokušala upotrijebiti istu novčanicu više puta ili u nekoliko transakcija. Ispravljanjem i tog nedostatka dobije se konačni oblik protokola.

3.2.3. Konačni oblik protokola

Konačni oblik protokola zadržava anonimnost kupca, ali samo do trenutka kada je ista elektronička novčanica upotrijebljena u dvije ili više transakcija. Tada (i samo

tada) je moguće identificirati kupca pomoću identifikacijske informacije koja se ugrađuje u elektroničku novčanicu.
Konačni oblik protokola plaćanja elektroničkim novcem ispunjava sve preduvjete za njegovu implementaciju: krivotvorenje novčanice se sprječava digitalnim potpisom banke u kojoj se nalaze bankovni računi kupca i trgovca, slijepi potpis s djelomičnim uvidom u sadržaj dokumenta osigurava anonimnost kupca, a višestruka potrošnja sprječava se mehanizmom identifikacijske informacije.

3.3. Komercijalni protokoli elektroničkog plaćanja

Razvojem Interneta počeli su se javljati mnogi prijedlozi za standarde elektroničkih plaćanja. Neki komercijalni sustavi koriste sustave kreditnih kartica, drugi čekove, treći obračunavaju kupnju preko telefonskog računa kupca itd. Čini se da najsvjetliju budućnost imaju sustavi elektroničkog plaćanja koji koriste e-gotovinu. Postoji (ili je postojalo) nekoliko komercijalnih sustava za elektroničko plaćanje, ovdje su spomenuti PayPal, CyberCash i eCash.

3.3.1. CyberCash

Tvrtka je bila osnovana 1994. godine i specijalizirala se poglavito za mikroplaćanja (engl. *micropayments*). Posao je s vremenom stagnirao i 2001. su proglasili stečaj.
Da bi se koristio CyberCash protokolom, kupac se morao koristiti klijent programom "The Wallet" koji je bio besplatan i mogao se jednostavno pribaviti i ugraditi, dok je trgovac morao imati svoj (trgovački) račun kod kompanije kreditnih kartica i svoj "terminal ID" za primanje Internet transakcija kod njihovih postojećih banaka.

3.3.2. eCash

eCash sustav je stvoren unutar tvrtke DigiCash, tvrtke pionira u području elektroničkog plaćanja koju je osnovao D. Chaum. DigiCash tvrtka je bankrotirala 1998. nakon čega ju je kupila tvrtka eCash Technologies.
eCash je skup protokola i metoda korištenih za obavljanje financijskih transakcija preko računarskih mreža poput Interneta. Protokol je baziran na korištenju "elektroničkih kovanica", tj. znakovnog niza koji sadrži podatke o vrijednosti, serijski broj dan od banke koja podržava eCash tehnologiju te digitalni potpis banke.
"Elektroničke kovanice" (1 eBuck = 1 USD) u transakcijama služe kao osnovna jedinica plaćanja. U slučaju da ne postoji dovoljan broj manjih kovanica, kupac zahtjeva od banke da mu razmijeni jednu veću na dvije manje kovanice od kojih jedna ima iznos isti kao račun koji treba podmiriti. Nakon obavljanja plaćanja, određeni broj digitalnih "kovanica" se prenosi preko Interneta, od kupca do trgovca. Krajnji rezultat je umanjivanje broja kovanica na disku kupca za plaćeni iznos i uvećavanje broja kovanica na disku trgovca.

3.3.3. PayPal

PayPal je jedini sustav u masovnoj primjeni. Omogućava pretvaranje novca s kreditne kartice ili bankovnog računa u e-novac, te slanje istoga e-poštom tvrtkama ili osobama primateljima u 55 zemalja svijeta (zasad ne i u Hrvatsku). Osim slanja e-novca, korisnici mogu stvoriti i virtualnu debitnu karticu, te plaćati direktno na račune u bankama. Broj korisnika je velik i danas je oko 100 milijuna, s izrazito brzim porastom. Veliki uspjeh PayPal-a leži u činjenici da se njihov koncept e-novca oslanja na postojeću infrastrukturu banaka i kreditnih kartica, te da mu je korištenje

jako jednostavno. PayPal e-novac se šalje e-poštom, vrlo jednostavno se pretvara u pravi novac (račun u banci, kreditna kartica i sl.), a neograničeno je prenosiv između fizičkih osoba, bez ikakve potrebe posjedovanja računa u banci, kreditne kartice i sl. Za transakcije e-novca preko PayPal-a dovoljno je samo imati adresu e-pošte.

Literatura

[1] http://os2.zemris.fer.hr/index.php?kat=84

[2] http://www.exeter.ac.uk/~RDavies/arian/emoney.html

[3] http://en.wikipedia.org/wiki/Electronic_cash

[4] http://www.virtualschool.edu/mon/ElectronicProperty/ElectronicMoney.html

[5] http://indomitus.net/2004status.html

[6] www.paypal.com

[7] Pavlić, I., SSL, Seminarski rad, FER Zagreb, 2005.