UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

RAZVOJ ELEKTRONSKIH PLAČILNIH SREDSTEV - STANJE V SLOVENIJI

Ljubljana, februar 2003 **JAKA LOBE**

IZJAVA

Študent Jaka Lobe izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom prof. dr. Borke Jerman-Blažič, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 5. 2. 2003. Podpis:

UVOD

Denar poznamo že zelo dolgo, ponekod so ga uporabljali že pred našim štetjem. Vedno je imel enak pomen, a se je njegova oblika skozi čas spreminjala. Kot vsaka druga stvar je tudi denar sledil razvoju. Sprva je bila njegova vrednost enaka teži kovine, iz katere je bil narejen, kasneje so ljudje ugotovili, da je to zelo nepraktično. Prišlo je do razvrednotenja denarja. Z razvojem komunikacijskih sredstev in pojavom interneta pa smo bili priča še dematerializaciji denarja, saj za nakup dobrin ni več potrebna fizična prisotnost denarja.

Poslovanje podjetij se je konec sedemdesetih let prejšnjega stoletja začelo spreminjati. S klasičnega načina poslovanja so podjetja počasi začela prehajati na elektronsko. To jim je omogočil razvoj računalniških omrežij in interneta ter združevanje informacijske in telekomunikacijske tehnologije. Sprva se je spremenil način poslovanja na finančnem trgu, saj so v sedemdesetih letih banke začele z elektronskimi finančnimi prenosi po varnih zasebnih omrežjih. Kasneje se je elektronsko poslovanje razširilo tudi v ostale panoge v obliki prenosa datotek, računalniške izmenjave podatkov in elektronske pošte. Elektronsko poslovanje, ki ga poznamo danes, se je dokončno razvilo v devetdesetih letih s pojavom svetovnega spleta.

S spreminjanjem oblik denarja in z razvojem elektronskega poslovanja pridemo do elektronskih plačilnih sistemov. Tako kot v vsakdanjem življenju se tudi tu srečujemo z različnimi oblikami elektronskih plačilnih sistemov. Tako poznamo elektronski denar, elektronske čeke in kovance ter plačilne in kreditne kartice. Poglavitna razlika med vsakdanjimi in elektronskimi plačilnimi sistemi je, da v elektronskem poslovanju vse poteka po elektronski poti in v nobeni fazi poslovanja ni fizične prisotnosti denarja.

Z razvojem mobilne tehnologije se odpira še eno področje za elektronske plačilne sisteme in sicer s pomočjo mobilnega telefona. Tako je Nova Ljubljanska banka v sodelovanju s podjetjem Mobitel v letu 2002 na slovenskem trgu prva predstavila storitev mobilnega bančništva – sistem Moba, leto prej pa je Mobitel predstavil sistem Moneta - plačevanje blaga in storitev s pomočjo mobilnega telefona. Lahko pričakujemo, da se bo sistem razvil v tri ločene storitve in sicer eMoneta za plačevanje majhnih in srednje velikih zneskov preko interneta, aMoneta za preprosto in hitro

brezgotovinsko plačevanje na raznovrstnih prodajnih avtomatih, ki so vključeni v mrežo storitve aMoneta, ter posMoneta za brezgotovinski nakup na prodajnih mestih, opremljenih s POS[1] terminalom.

V diplomski nalogi bom predstavil elektronske plačilne sisteme, njihov razvoj ter razširjenost. Predstavil bom tudi stanje elektronskih plačilnih sistemov v Sloveniji in podrobneje predstavil sistema Moba in Moneta. Pri preučevanju elektronskih plačilnih sistemov si bom pomagal z literaturo in informacijami z interneta ter z lastnimi izkušnjami pri plačevanju blaga in storitev prek interneta. Za predstavitev sistemov Moba in Moneta bom uporabil informacije, ki jih Nova Ljubljanska banka in Mobitel z reklamnimi brošurami, navodili ter internetnimi stranmi nudita uporabnikom. V diplomski nalogi bom pri prikazu osnov elektronskega poslovanja uporabil nekatere kratice in angleške izraze, ki so postali veljavna imena v strokovnem jeziku interneta. Razlaga in slovenski prevod bo v slovarju, ki je del priloge.

1. KRATKA ZGODOVINA INTERNETA

Zametki interneta segajo v šestdeseta leta prejšnjega stoletja. Sprva so bili ti sistemi prekompleksni in zato dostopni le ozki množici strokovnjakov. Ustanovitev agencije ARPA[2], ki so jo Američani ustanovili leta 1957 zaradi izstrelitve prvega ruskega satelita, predstavlja prvo dejanje v razvoju interneta. Ideja je bila povezati računalnike brez neke sredinske točke. Tako je nastala mreža ARPANET, ki je povezovala računalnike univerz v Los Angelesu, Santa Barbari, Standfordu in Utahu. Prvič so to povezavo vzpostavili 29. oktobra 1969. Z leti so se v to mrežo priključevala še druga univerzitetna središča. Prvo neameriško vozlišče, ki se je povezalo v ARPANET, je bilo leta 1973 v Londonu. V tem času so postavili že standard za danes nepogrešljivo elektronsko pošto. Prav tako so že postavljali zasnove za protokol za prenos datotek. V sedemdesetih letih so se pojavili prvi zaprti omrežni medbančni sistemi. V prvi polovici osemdesetih let se je do konca razvijal tudi TCP/IP[3] protokol. V zgodnjih osemdesetih letih so prva podjetja že uvedla elektronsko poslovanje, saj so prek omrežij izvajala prenos datotek, računalniško izmenjavo podatkov ter elektronske pošte. Prva registrirana domena je bila Symbolics.com, ki

[1] *Point Of Sale*
[2] *Advanced Research Projects Agency*
[3] *Transmision Control Protocol/Internet Protocol*

je bila registrirana leta 1985. Takrat so tudi vzpostavili krovne domene .com, .net, .org, .edu ter .uk. . V tem času se je pojavila tudi storitev klepetalnic (IRC[4]). Devetdeseta leta so prinesla dokončno uveljavitev interneta s pojavom svetovnega spleta, saj je leta 1991 Tim Barners - Lee izumil protokol za svetovni splet (WWW)[5], na katerem temeljita internet in protokol za prenos teksta in slik (HTTP[6]). Od takrat naprej se internet samo še širi, in če smo na začetku lahko prešteli sodelujoče strežnike, je v današnjem času to praktično nemogoče. Z razvojem komunikacijskih sredstev se je večalo tudi število uporabnikov, prav tako pa tudi hitrost prenosov,vsebina ter ponudba.

2. ELEKTRONSKO POSLOVANJE

Verjetno si večina ljudi ob izrazu elektronsko poslovanje predstavlja, da gre tu predvsem za internetno stran, ki reklamira določen proizvod, vsebuje informacije za naročila in ima morda še možnost on-line plačila. To pa seveda ni vse. Elektronsko poslovanje pomeni, da so podjetja s pomočjo računalnikov in informatizacije procesov posodobila del ali celotno poslovanje, kot na primer komunikacijo z dobavitelji in odjemalci, skladiščenje, distribucijo, trženje, prodajo, ipd. Vendar je elektronska trgovina le del elektronskega poslovanja podjetja. Poznamo elektronsko poslovanje med podjetji in posamezniki (elektronska trgovina, elektronsko bančništvo), elektronsko poslovanje med podjetji (trgovanje) in elektronsko poslovanje med posameznikom in državnimi ustanovami (sodelovanje na razpisih, napoved dohodnine, ipd).

Podjetja stremijo k uspešnemu poslovanju in le-to dandanes ni več možno brez ustreznega informacijskega sistema. Če želi podjetje elektronsko poslovati, mora spremeniti strukturo podjetja in na novo opredeliti osnovne modele poslovanja z moderno tehnologijo. Podjetja se za to odločajo, da bi izboljšali učinkovitost poslovanja, ki jo občutijo tako stranke podjetja kot podjetje samo. S prehodom na elektronsko poslovanje podjetja predvsem skrajšajo čas določenim operacijam, imajo lažje dostopne in natančnejše informacije o stanju podjetja in zmanjšajo stroške, saj zaradi uporabe računalnikov in interneta zmanjšajo porabo pisarniškega materiala, poštnih storitev, hkrati pa ni več potrebna njihova

[4] *Internet Relay Chat*
[5] *World Wide Web*
[6] *Hyper Text Transfer Protocol*

fizična prisotnost, zato se izognejo stroškom odpiranja poslovalnic ter najema ali nakupa poslovnih prostorov. Z vstopom na globalni trg se podjetjem število potencialnih strank ter poslovnih partnerjev drastično poveča, saj je razvoj interneta prišel že tako daleč, da danes praktično ni več možno prešteti vseh strežnikov, ki so povezani v svetovni splet. Tako lahko o številu uporabnikov interneta le ugibamo. Po nekaterih podatkih (URL:http://www.glreach.com/globstats/), 2002) je bilo marca leta 2002 po svetu nekje med 560 in 580 milijonov rednih uporabnikov interneta. Tabela 1 prikazuje število uporabnikov po posameznih kontinentih.

Tabela 1: Število uporabnikov interneta po svetu

Kontinent	Število uporabnikov (v mio)
Evropa	185.83
ZDA in Kanada	182.67
Južna Amerika	32.99
Afrika	6.31
Srednji vzhod	5.12
Azija/Pacifik	167.86
Skupaj	580.78

Vir: NUA Internet surveys, 2002.

Temu številu je potrebno dodati še neocenljivo množico priložnostnih internetnih deskarjev. Glede na trend povečanja števila uporabnikov vsako leto v letu 2003 lahko pričakujemo 760 milijonov uporabnikov, kar pomeni 30 odstotno povečanje števila uporabnikov svetovnega spleta.

2.1. KAKO ZAČETI Z ELEKTRONSKIM POSLOVANJEM

Ko se podjetje odloči za elektronsko poslovanje, mora dobro izračunati stroške za uvedbo, zagotavljanje varnosti in za prestrukturiranje poslovanja, saj je moč izbrati več različnih kombinacij. Vse je odvisno od trenutnega stanja podjetja in njegove okolice. Podjetje mora ugotoviti, kakšne so lahko njegove bodoče konkurenčne prednosti v digitalnem poslovnem svetu. Preživetje podjetja je predvsem odvisno od sposobnosti predvidevanja, ocenjevanja in odzivanja na spremenljive potrebe kupcev, potrošnikov, dobaviteljev ter partnerjev v poslovanju. Tako se je treba na spremembe pripraviti in jih nato tudi izpeljati.

Napotki podjetjem, ki želijo začeti elektronsko poslovati, izdelani po analizi v Evropski uniji (URL:http://europa.eu.int/ISPO/ecommerce/MoU/), 2002), kažejo pet ključnih dejavnikov uspeha:

- *vsebina, ki jo podjetje nudi na spletu*. Podjetje naj ponudi izdelek ali storitev, ki je inovativna in jo je moč tržiti po internetu;
- *pripravljenost podjetja, da se pojavi na globalnem trgu*. Za uspešno elektronsko poslovanje ni dovolj le vstop na svetovni splet, ampak so potrebne še investicije v dodatno trženje in oglaševanje;
- *nadzor in upravljanje v podjetju*. Za uspešno uvedbo elektronskega poslovanja je potrebna temeljita reorganizacija poslovanja, da ne pride do podvajanja operacij za elektronski in klasičen način poslovanja;
- *okolje podjetja, ki zagotavlja kritično maso potrošnikov in poslovnih partnerjev*. Ko podjetje uvaja elektronsko poslovanje in trgovanje preko spleta, mora poskrbeti, da bodo nov način poslovanja sprejeli tudi njegove stranke in poslovni partnerji;
- *tehnologija za elektronsko poslovanje*. Podjetje mora zakupiti in obvladati tehnologijo, primerno njegovemu obsegu dela. Vzorec je pokazal, da ravno pomanjkanje znanja in informacij po navadi vpliva na to, da podjetja ne uporabljajo sistemov za plačevanje po internetu z vgrajenimi varnostnimi mehanizmi. Brez tega pa ostajajo na ravni reklamnega kataloga.

Večina podjetij elektronsko posluje preko svetovnega spleta, nekatera pa se odločijo za postavitev ekstraneta[7]. To zahteva še večje stroške in poznavanje tehnologije, zato je najbolj primeren le za srednje velika in velika podjetja. Najpomembneje je , da je ekstranet uspešen le takrat, ko podjetju uspe prepričati svoje poslovne partnerje za njegovo uporabo, ki morajo z vključitvijo v ekstranet spremeniti svoje poslovne sisteme. Prednost ekstraneta je v še krajšem času med naročilom, dobavo in plačilom izdelkov ali storitev. Poleg tega prihaja tudi do zmanjšanja obratovalnih stroškov.

2.2. POSLOVNE FUNKCIJE IN ELEKTRONSKO POSLOVANJE

Uvedba elektronskega poslovanja in pojava na svetovnem spletu za podjetje pomeni spremembo tako notranjih kot zunanjih poslovnih

[7] *Lokalno omrežje, ki omogoča omejeno dostopnost tudi od zunaj. Omejitve dostopa so po navadi določene z uporabniškimi imeni in gesli. Zelo je priljubljen za izmenjavo informacij med poslovnimi partnerji.*

operacij. Za notranje delovanje podjetja elektronsko poslovanje ponuja raznovrstna orodja za pretok informacij, za sodelovanje in razvoj, za podporo odločanju ter za vodenje poslovnega procesa pri dobavi in prodaji. Ti sistemi podjetju omogočajo učinkovitejše in donosnejše delovanje. Pri zunanjih operacijah se elektronsko poslovanje največkrat vidi kot trženje in kot spletna trgovina z vsemi funkcijami, kot so informiranje, podpora strankam, naročanje, plačevanje, spremljanje naročil in podobno. Predvsem pa daje medmrežje možnost podjetju za vzpostavitev sistema za upravljanje odnosov s strankami in kupci, kar je za uspešno poslovanje podjetja zelo pomembno.

Trženje in komuniciranje s strankami podjetja
Internet nudi podjetju učinkovite instrumente za vzpostavljanje navideznih osebnih odnosov s strankami. Ena od značilnosti interneta je, da je moč potrošnikom predstaviti lahko dostopne in dobro pripravljene informacije. Prednost komuniciranja s strankami prek interneta je tudi multimedia[8], s čimer se v potrošniku vzbudi zanimanje za izdelke, poleg tega pa mu omogoči, da se z njim dobro seznani. Potrošniki cenijo predvsem kakovostne in izbrane informacije o izdelkih in poslovni dejavnosti podjetja. Predstavitev na svetovnem spletu tako podjetjem daje možnost, da objavijo toliko informacij, kot mislijo, da je potrebno. Informacije o namenu izdelka, načinu uporabe ali storitve lahko prepričajo kupca za njegov nakup in tako povečajo prodajo in s tem dobiček podjetja. Za razliko od ostalih medijev oglaševanja je svetovni splet v celoti dvosmeren in tako lahko podjetje dobi tudi povratne informacije od potrošnikov.

Na internetu poznamo več oblik metod oglaševanja in trženja:

- *lastna spletna stran*: obstaja nešteto različnih receptov za izdelavo dobrih in uspešnih spletnih strani. Podjetje mora izbrati tako, ki bo primerna vsebini, ki jo želi podati, in bo pritegnila ciljno populacijo;
- *elektronska pošta*: z elektronsko pošto lahko podjetje direktno oglašuje posamezno spletno stran ali blagovno znamko. Čeprav uporabniki večkrat niso zadovoljni s takšnim načinom oglaševanja, se večina podjetji zateče k temu, saj je najcenejša oblika oglaševanja z možnostjo slikovne in grafične predstavitve;
- *reklamni oglasi*: pasice ali reklamni oglasi so območja na spletnih straneh, ki nimajo direktne povezave z vsebino strani, vendar

[8] *večpredstavnost*

reklamirajo neko drugo stran, na katero pridemo s klikom na reklamni oglas. Obstajajo specializirane spletne strani, ki "zbirajo" reklamne oglase in jih združujejo po kategorijah. Lahko pa si podjetja reklamne oglase preprosto izmenjajo;

- *indeksiranje strani za znane spletne iskalnike*: iskalnik je programska oprema, postavljena na določenih strežnikih interneta, ki indeksira naslove spletne strani na podlagi njihove vsebine, - neke vrste imenik spletnih strani. Tako uporabniki, ki ne vedo točnega naslova, vedo pa, kaj iščejo, vpišejo ključne besede v določen iskalnik in ta jim izpiše spisek strani, ki vsebujejo opisane ključne besede;
- *portali*: portali podobno kot iskalniki nimajo svoje lastne vsebine, ampak imajo zbirko kategoriziranih povezav na ostale spletne strani. Portali in iskalniki so najpogostejše obiskane spletne strani in se zato pogosto uporabljajo kot oglaševalci.

Odnosi s strankami, prodaja, dobava in logistika

Posledice uvajanja elektronskega poslovanja in globalizacije industrije in trgovine so pripeljale do večje specializacije v poslovanju in izkoriščanju ekonomije obsega, zmanjševanja števila dobaviteljev ter centraliziranega nadzora zalog, skladiščenja in distribucije. Čas dobave se je skrajšal do minimuma in v nekaterih primerih znaša le še 24 ur. Hitrost in optimizacija dobave vpliva na zmanjševanje stroškov.

Odnosi s strankami

Sodobna tehnologija za svetovni splet omogoča natančno spremljanje dogajanj na mreži in zbiranje informacij o uporabnikovih navadah. Veliko podjetij ponudi uporabnikom ob prvem obisku, da se registrirajo na njihovi spletni strani. Obenem jim zastavijo nekaj splošnih vprašanj. S programsko opremo lahko tudi sledijo uporabnikom, kako se premikajo skozi spletno aplikacijo. Tako pridobljene informacije pomagajo marketinškemu oddelku podjetja razumeti, kaj imajo ljudje radi, kako se po spletnih straneh premikajo, kam in kako je potrebno postaviti oglase in kakšne informacije ljudje iščejo. Analiza podatkov lahko opredeli posamezne trge, identificira posamezne skupine kupcev na trgu in diferencirajo posamezne demografske in psihografske skupine kupcev s tem, da priskrbijo vpogled v način, kako se posamezni uporabniki odločajo za nakupe. Tako so podjetja sposobna ponuditi prilagojeno komunikacijo, poosebljeno storitev in izdelke, prilagojene posamezniku. Podjetja z dobro urejenimi odnosi s strankami prihrani pri oglaševanju in trženju. Poleg

tega pa lahko tako zbrane informacije pripomorejo k izboljšanju izdelka, storitve ali pa interaktivne informacije, ki ustreza potrebam potrošnika.

Gradnja odnosov s strankami ima cilj pridobiti nove stranke, izboljšati in vzdrževati odnose z obstoječimi strankami, zato mora biti center aktivnosti podprt z vso razpoložljivo tehnologijo, kot so telefon, fax, spletna stran in elektronska pošta. Na tak center se potem lahko navežejo še ostale funkcije informacijskega sistema, kot so vzdrževanje baze kupcev, podpora uporabnikom, servis, trženje in tržne raziskave, prodaja in podobno.

Prodaja
Z uvedbo elektronskega poslovanja mora podjetje poskrbeti, da integrira prodajno funkcijo v okvire centralnega informacijskega centra. Tako neposredno poveže prodajo s proizvodnjo, informacijami o stanju zalog ter informacijami o naročilih. Kupec lahko v vsakem trenutku vidi, kakšen je dobavni rok za določeno blago ter kakšno je stanje naročenega blaga. Prodaja posameznega izdelka se avtomatično ažurira v bazi podatkov, tako se v bazi v vsakem trenutku vidi, kakšno je dejansko stanje na policah trgovin, zalog v skladiščih ter distribucijskih centrih. Tako se skrajša čas od naročila do dobave in ne prihaja do primerov, ko izdelka ali storitve zmanjka.

Dobava
Dobavna veriga je sestavljena iz procesov, ki pridobivajo, transformirajo, skladiščijo in prodajajo surovine, vmesne ter končne proizvode. Po navadi je sestavljena iz več podjetij, ki pa niso tako učinkovita kot eno večje, saj si do nedavnega niso mogla dovolj hitro izmenjavati informacij o pretoku blaga. Novejše aplikacije za elektronsko poslovanje so omogočile, da tudi na tem področju pride do optimizacije. Tako sedaj podjetja lahko porazdelijo kapacitete izdelave in distribucije na najbolj optimalne lokacije po svetu in niso več lokalno omejena. Tradicionalni način vodenja zalog in logistike izginja, ker kupci zahtevajo hitrejše odgovore na povpraševanje. Transport se internacionalizira. S pomočjo programske opreme podjetja lahko načrtujejo stanja zalog, števila naročil, distribucijo, transport in podobno. Pri izvedbi pa podjetje poskrbi za upravljanje s pretokom blaga skozi distribucijske centre in skladišča ter z nadzorom zagotavlja, da so izdelki dobavljeni na pravi naslov ob izbiri najboljšega transporta, ki je na voljo. Dobra dobava zahteva avtomatizirana skladišča in upravljanje dostavnih vozil.

3. VARNOST V ELEKTRONSKEM POSLOVANJU

Ker v elektronskem poslovanju ni fizične prisotnosti stranke in prodajalca, informacije pa se pretakajo po računalnikih in omrežjih, morajo podjetja poskrbeti za varnost teh podatkov. Poleg tega morajo preprečiti ponarejanje informacij, pretvarjanje, nepooblaščeno uporabo virov, nepooblaščeno razkritje informacij, zanikanje sodelovanja pri določenih dejavnostih, onemogočanje dela oziroma uporabe virov ter analizo prometa. Glede na določene raziskave je moč ugotoviti, da je pomanjkanje varnosti po mnenju uporabnikov največja ovira za večji razmah elektronskega poslovanja. Pri obravnavi varnosti je vedno potrebno upoštevati vire, ki imajo za njihove lastnike določeno vrednost, nevarnosti, ki pretijo virom, možne ranljivosti in napade ter načine realizacije groženj, učinke uresničevanja groženj na vire ter varnostne ukrepe za zaščito virov.

Poznamo več vrst virov, ki jih mora varnostna infrastruktura podjetja zaščititi pred zmanjševanjem vrednosti. Najpomembnejši so podatki ali informacije pri prenosu in hranjenju. Tu so še programska in strojna oprema, uporabniki ter odnosi med njimi, dokumentacija o postopkih in strojni ali programski opremi v sistemu ali omrežju. Prav tako poznamo več oblik groženj: notranje in zunanje, namerne in nenamerne. Uporabniki storitev elektronskega poslovanja od podjetja pričakujejo, da bo zagotovilo potrebno varnost poslovanja ter da bodo storitve stalno prisotne in na voljo. Da bi zadovoljilo varnostim zahtevam uporabnikov, mora podjetje uvesti sistem, ki bo omogočal naslednje varnostne storitve:

- *overjanje*: vsak mora imeti možnost preverjanja identitete subjektov, s katerimi komunicira, in izvor podatkov;
- *zaupnost*: določene informacije ne smejo biti razkrite nepooblaščenim subjektom;
- *neokrnjenost*: podatki morajo biti zaščiteni pred nepooblaščenim spreminjanjem;
- *nadzor dostopa*: preprečevanje nepooblaščene uporabe določenih sredstev;
- *preprečevanje zanikanja*: preprečevanje možnosti zanikanja sodelujočih subjektov, da so v določeni aktivnosti dejansko sodelovali;
- *razpoložljivost*: storitev elektronskega poslovanja morajo biti stalno na voljo.

Za zagotavljanje teh varnostnih storitev je na voljo več metod. Izbira metode je odvisna od zahtevanih varnostnih storitev, stopnje zaščite in vrste sistema. Na lokalni ravni se je za najbolj učinkovito metodo izkazala fizična izolacija sistemov z zaupnimi informacijami. Vendar pa elektronsko poslovanje poteka preko javnih omrežij in taka metoda zato ni primerna. Za varovanje podatkov v elektronskem poslovanju se uporablja šifriranje. Za preverjanje identitete se največkrat uporabljajo navadna ali enkratna gesla in različni kriptografski protokoli. Nadzor dostopa je mogoče zagotoviti s seznami. Preprečevanje zanikanja sodelovanja pri aktivnostih pa dosežemo z digitalnimi podpisi, ki nadomestijo običajne.

3.1. ŠIFRIRANJE

Spreminjanje podatkov (čistopisa) v obliko, ki onemogoča njihovo razumevanje in ohranja tajnost (tajnopis), imenujemo šifriranje. Obratni proces pa dešifriranje. Za obe transformaciji so pomembni postopek zakrivanja in razkrivanja (kriptografski algoritem) in šifrirni ključi, ki določajo delovanje algoritma. Modernejši algoritmi so večinoma do podrobnosti znani vsakomur, za uspešno varovanje podatkov morajo skriti ostati le šifrirni ključi. Vsi našteti elementi, skupaj z vsemi možnimi tajnopisi in podatki, ki jih lahko zaščitimo, sestavljajo kriptografski sistem (kriptosistem). V grobem ločimo kriptosisteme na simetrične in asimetrične.

Simetrični kriptosistemi za šifriranje in dešifriranje uporabljajo isti ključ. Zato prihaja v javnih omrežjih do problema, kako šifrirni ključ varno razdeliti pooblaščenim subjektom. Vsaj pred začetkom prve vzpostavitve si morajo tako subjekti šifrirni ključ osebno izmenjati, kar je dandanes, ko komuniciramo lahko po vsem svetu, nesprejemljiv postopek, če ljudi nadomeščajo računalniki pa nemogoč postopek. Druga slabost simetričnih kriptosistemov je tudi število ključev, saj moramo imeti toliko ključev, kolikor je subjektov, s katerimi komuniciramo. Simetrični algoritmi se zaradi svojih slabosti uporabljajo v kombinaciji z drugimi algoritmi, ki omogočajo varno izmenjavo ključev ali pa v manjših skupinah ljudi, kjer problem upravljanja ključev ni tako velik.

V *asimetričnih kriptosistemih* imamo dva ključa. Tu ključ za šifriranje ni enak ključu za dešifriranje. Najpomembnejša lastnost takih kriptosistemov je, da iz enega ključa brez poznavanja dodatnih informacij ni mogoče določiti drugega. Zaradi te lastnosti lahko en ključ javno objavimo. Tak

ključ imenujemo javni ključ, drugi ključ, ki ga mora lastnik varno spraviti, pa zasebni ključ. Če nam nekdo želi poslati zaupno sporočilo, ga šifrira z našim javnim ključem. Samo mi, ki edini poznamo ustrezni zasebni ključ, lahko šifrirano sporočilo dešifriramo. V asimetričnih kriptosistemih imamo za razliko simetričnih kriptosistemov ne glede na število subjektov, s katerimi komuniciramo, le en par ključev. Slabost asimetričnih kriptosistemov v primerjavi s simetričnimi je v tem, da so veliko počasnejši, zato jih ne uporabljamo za šifriranje daljših sporočil. Običajno za šifriranje podatkov uporabljamo simetrične kriptoalgoritme, ključe za te algoritme pa šifriramo z asimetričnimi kriptoalgoritmi. Kriptosisteme javnih ključev torej uporabljamo pri šifriranju večinoma le za razdeljevanje ključev.

3.2. VARNOST ŠIFRIRNIH ALGORITMOV

Za najbolj znane in preizkušene simetrične kriptografske sisteme velja predpostavka, da ne vsebujejo nikakršnih varnostnih lukenj, zato se napadalec lahko loti dešifriranja le na ta način, da izmed vseh možnih ključev s poskušanjem najde pravega. Zato je za varnost pomembno, da je velikost in s tem tudi število možnih ključev čim večja. Najbolj znan simetrični kriptoalgoritem je DES[9], ki ima ključe velike le 40 bitov. Zato ni več varen. Zaželeno je, da pri simetričnemu šifriranju uporabljamo le preizkušene simetrične algoritme z najmanj 72 bitov dolgimi ključi. To pomeni, da je vseh ključev 2^{72}. Algoritem IDEA[10] uporablja ključe velikosti 128 bitov. Preverjanje vseh ključev pri algoritmu IDEA bi s precej zmogljivim računalnikom, vrednim nekaj milijonov dolarjev, trajalo več tisoč let. Poleg IDEA algoritma se največkrat uporabljajo še trojni DES, Blowfish in pa naslednik DES, sistem AES[11].

Za razbitje asimetričnih kriptografskih algoritmov obstajajo poleg preizkušanje vseh možnih ključev tudi druge metode. Kljub temu je število ključev še zmeraj najpomembnejša informacija, a samo na tej osnovi ni mogoče direktno primerjati simetričnih in asimetričnih kriptografskih algoritmov. Po primerjalni tabeli, ki sta jo pripravila Lenstra in Verhuel (URL:http://www.tbtf.com/archive/1999-12-16.html), 2002), je moč

[9] *Data Encrypton Standard*
[10] *International Data Encrypton Algorithm*
[11] *Advanced Encryption Standard*

ugotoviti, da velikost 1028 bitov pri RSA[12] pomeni podobno stopnjo varnosti kot 72 bitov dolgi ključi pri simetričnih algoritmih.

Zaradi kakovostnih kriptosistemov se ponavadi tisti, ki se želijo dokopati do zaupnih dokumentov, ne odločajo za razbitje znanih algoritmov, ampak raje poizkušajo najti šibkejše točke, kot recimo napačno konfiguracijo sistema ali napake v programski opremi. Zato je pomembno, da si podjetja zagotovijo varnostne sisteme v vseh sistemih, ki sodelujejo pri poslovanju. Prava velikost ključev in izbira preizkušenih algoritmov je samo potreben pogoj za varno elektronsko poslovanje, ni pa tudi zadosten.

3.3. ELEKTRONSKI PODPIS

Namesto lastnoročnega podpisa poznamo v elektronskem poslovanju elektronski podpis. Namenjen je preverjanju pristnosti podatkov in identifikaciji podpisnika. Dokument je lahko podpisan s sliko lastnoročnega podpisa, pripeto k dokumentu, lahko je podpisan z elektronskim peresom ali na podlagi simetričnih kriptografskih algoritmov. Vendar so te metode preveč enostavne za zahtevano stopnjo varnosti. Zato se za elektronsko podpisovanje uporablja digitalni podpis, ki temelji na asimetrični kriptografiji in zagotavlja neokrnjenost dokumenta. Tak podpis je odvisen od vsebine dokumenta in vsaka najmanjša sprememba povzroči, da podpis ni veljaven, zato tudi ni nevarnosti, da bi nekdo prekopiral originalni podpis in z njim podpisoval druge dokumente. Preprečuje tudi možnost zanikanja, saj je praktično nemogoče prirediti zasebni ključ, ki je znan le njegovemu lastniku, zato lahko identiteto podpisnika vsakokrat popolnoma preverimo.

Tudi za digitalno podpisovanje obstaja več metod, izbira pa je odvisna od zahtev uporabnika in širšega okolja. V glavnem se uporablja algoritem RSA v kombinaciji z enosmernimi zgoščevalnimi funkcijami. Podpisovanje poteka v dveh korakih. Podatke najprej skrčimo z eno od enosmernih zgoščevalnih funkcij, ki poljubno dolgo besedilo preslikajo v blok konstantne dolžine. S tako zgostitvijo uničimo informacije, ki jih nosi dokument, zato prvotnih podatkov ni moč ponovno rekunstruirati. Dobljeni blok, ki predstavlja besedila, nato šifriramo s svojim zasebnim ključem in tako dobimo digitalni podpis. Pri preverjanju najprej

[12] *Imenovan po njegovih avtorjih: Rivestu, Shamirju in Adlemanu*

dešifriramo podpis z javnim ključem podpisnika, nato sami izračunamo vrednost enosmerne zgoščevalne funkcije podpisanih podatkov in primerjamo bloka. Če se ujemata, je podpis pravi, če pa ne, je dokument podpisal nekdo drug ali pa se je vsebina dokumenta od časa podpisa spremenila.

3.4. DIGITALNI CERTIFIKAT

Pred uporabo javnih ključev moramo biti povsem prepričani, da ključ res pripada naslovniku šifriranega sporočila oziroma domnevnemu podpisniku sporočila. Overjanje javnih ključev je zato temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetrični kriptografiji. Preverjanje povezave med uporabnikom in njegovim ključem omogočajo posebne ustanove, imenovane *overitelji* oziroma agencije za certificiranje javnih ključev (AC). Overitelj izda lastniku javnega ključa digitalno podpisano potrdilo, imenovano digitalni certifikat, s katerim zagotavlja drugim uporabnikom avtentičnost ključa in s pomočjo tega certifikata lahko lastnik dokaže lastništvo ključa in s tem tudi svojo identiteto.

Preverjanje digitalnih podpisov in neokrnjenost potrdil je lažji del overjanja javnih ključev, saj poteka povsem avtomatično. Težji del je odločanje, v kolikšni meri lahko zaupamo posameznim agencijam za overjanje, če je bila identiteta imetnikov ključev dovolj preverjena za določen namen uporabe in če se v določeni situaciji ključ sploh sme uporabiti. Poznamo namreč več različnih agencij, ki overjajo ključe za različne namene. Večina je komercialnih (Verisign) ali namenjena državni upravi. Ena redkih infrastruktur, katerih namen je združevanje overiteljev iz različnih držav, je EuroPKI. Vzpostavljena je bila v projektih Evropske unije z namenom zagotavljanja varnostnih storitev za območje celotne Evrope. Del infrastrukture, katere vrhovna agencija ima sedež v Torinu, je tudi slovenska agencija za certificiranje SI-CA, ki podpisuje ključe drugih slovenskih overiteljev, posameznikov in spletnih strežnikov organizacij. V Sloveniji so ustanovile svoje agencije še Center vlade za informatiko, Trade Point Slovenija in nekatere komercialne organizacije. Za potrebe identifikacije svojih strank pri elektronskem bančništvu izdaja certifikate tudi Nova Ljubljanska banka.

3.5. POSTOPKI ZA PREVERJANJE IDENTITETE

Preverjanje vira podatkov nam omogoča digitalni podpis, za ugotavljanje

resnične identitete sogovornikov pa uporabljamo protokole overjanja. Identiteto uporabnika lahko preverimo na podlagi nečesa, kar uporabnik ve, oziroma na podlagi njegovih fizičnih lastnosti. Najenostavnejši način je šibko overjanje, kjer je identiteta določena s poznavanjem gesla oziroma določene informacije. Geslo enolično določa uporabnika takrat, ko je znan le njemu. Šibko overjanje s pomočjo gesel zaradi svojih pomanjkljivosti ni primerno za identifikacijo v elektronskem poslovanju, razen za dostop do lokalnega sistema ali aktiviranje določenih naprav, na primer pametnih kartic. Ranljivost gesel v nezavarovanih omrežjih lahko zmanjšamo z enkratnimi gesli. Prisluškovanje tu nima pravega pomena, saj je geslo veljavno le za trenutno povezavo in ob ponovni povezavi ne bo več veljavno. V nadzorovanem okolju je boljši način preverjanje identitete na podlagi biometričnih lastnosti (prstni odtis, očesna roženica). V tem primeru se uporabnik identificira z nečim, kar je, in ne s tistim, kar ve.

3.6. VARNOSTNE APLIKACIJE IN PROTOKOLI

Sistemi za identifikacijo z uporabo enkratnih gesel so odporni na prisluškovanje in prestrezanje (pasivni napadi), niso pa na aktivne napade, kjer napadalec aktivno spreminja podatke z vstavljanjem novih ali spreminjanjem obstoječih. Protokoli, ki tudi na te napade niso občutljivi, so sestavljeni iz več korakov in večinoma uporabljajo kriptografske mehanizme, najpogostejše digitalne podpise. Prednost teh metod je tudi ta, da nobena izmed sodelujočih strani pri overjanju ne dobi dovolj informacij, da bi se lahko kasneje izdajala za nasprotno stran.

Za zaščito transakcij v svetovnem spletu se najpogosteje uporabljajo protokoli SSL[13], TLS[14] in WTLS[15]. Bistvo vseh postopkov je, da vzpostavijo varen kanal med strežnikom in odjemalcem, na primer spletnim brskalnikom. Vsem informacijam, ki potujejo po takšnem kanalu, je lahko zagotovljena zaupnost, neokrnjenost in avtentičnost izvora.

3.7. VARNA ELEKTRONSKA POŠTA

Varna izmenjava elektronskih sporočil je osnova za vsakršne oblike elektronskega poslovanja. Za varno elektronsko poslovanje s subjekti z vsega sveta je bistven enoten standard, ki določa obliko sporočil, način

[13] *Secure Sockets Layer*
[14] *Transport Layer Security*
[15] *Wireless Transport Layer Security*

zaščite in potrebno infrastrukturo. Takšen standard za varno elektronsko pošto na internetu se imenuje S/MIME[16]. Ta omogoča overjanje pošiljatelja, neokrnjenost sporočil, zaupnost sporočil in preprečevanje zanikanja avtorstva. Dodatne zahteve varne elektronske pošte mora izpolniti sistem za prenos pošte, saj jih ni mogoče zagotoviti v aplikaciji sami.

Za zaščito elektronske pošte se pogosto uporablja program PGP[17]. PGP je program, ki lahko zagotovi zaupnost, neokrnjenost in overjanje sporočil. Priljubljenost med uporabniki je dosegel s tem, da je že od nastanka zastonj, enak po vsem svetu in enostaven za uporabo.

Vse opisane varnostne metode in sistemi pa niso dovolj za varno elektronsko poslovanje, če podjetje ne poskrbi za varnost svojih baz podatkov in strojne opreme, ki sodeluje pri elektronskem poslovanju. Pred vdorom vsiljivcev in nepovabljenih se mora vsako podjetje zaščititi s požarnim zidom, ki ga lahko najdejo tudi brezplačno na internetu, ali pa kupijo profesionalni sistem znanih proizvajalcev računalniške opreme. Vsi sistemi zagotavljajo varnost in fleksibilnost omrežnega sistema in preprečujejo ne avtorizirano pregledovanje podatkov na trdih diskih. Brez zagotovitve take varnosti je za podjetje nesmiselno, da začne kakršnekoli aktivnosti v zvezi s spletnim ali elektronskim poslovanjem. Podjetje določi potrebe po varnosti in tehnične rešitve na podlagi ocene možnosti zlorab in ostalih tveganih posegov.

4. ELEKTRONSKI PLAČILNI SISTEMI

V vsakdanjem življenju smo navajeni, da blago ali storitve plačujemo z različnimi plačilnimi sredstvi. Oblike plačilnih sredstev se v skladu s tehnologijo spreminjajo. Od nekdaj je pri plačevanju prisotna gotovina, kasneje so se pojavili čeki, ki pa so jih izrinile kreditne in bančne kartice. Podjetja že tradicionalno med seboj poslujejo elektronsko, vendar so med seboj uporabljala zasebna omrežja, narejena posebej za to priložnost (bančno omrežje, omrežje mednarodnega združenja letalskih prevoznikov ipd). Z razmahom elektronskega poslovanja se je razširilo tudi elektronsko plačevanje v odprtih omrežjih. Razlike med klasičnim in elektronskim poslovanjem niso velike, saj imata oba enako poslovno logiko. Glavna

[16] *Secure/Multipurpose Internet Mail Extensions*
[17] *Pretty Good Privacy*

razlika je le v tem, da na omrežju stranke, ki nekaj kupujejo, uporabljajo računalnik in spletni brskalnik, trgovec, ki nekaj prodaja, pa spletni strežnik. Stranka preko brskalnika opravi naročilo in pove, na kakšen način bo plačala.

Tudi v elektronskem poslovanju poznamo več oblik plačil, in sicer plačilo s kreditno kartico, z elektronskim denarjem, z elektronskim čekom, z elektronskim prenosom nakazila, na kredit ipd. Na strani prodajalca mora strežnik dokončati posel tako, da preveri zaloge in avtorizira prenos sredstev od naročnika k prodajalcu. To poteka ponavadi s pomočjo posebnih naprav za povezavo med prodajalcem in banko prek interneta ali prek zasebnega bančnega omrežja, podobno kot pri navadnih prodajalnih terminalih.

Poleg osnovnih parametrov za zagotovitev varnosti, ki se zahtevajo od plačilnega sistema, obstaja še vrsta drugih parametrov, ki zagotavljajo, da je elektronsko plačevanje podobno klasičnemu:

- vrsta plačila: kreditno (odloženo plačilo), predplačilo in elektronski denar (plačilo takoj);
- neposredni dostop do plačilnega sistema (on-line) ali dostop do prodajnega mesta (off-line);
- vrsta zahtevane opreme: kartice, elektronske denarnice, čitalniki pametnih kartic ipd.;
- prisotnost ali neprisotnost stranke ali vmesnega plačila za avtorizacijo plačil;
- mikroplačila (nekaj 1000 sit), makro plačila (nekaj tisoč EUR) oziroma velikost dovoljene transakcije;
- odgovornost in zaupanje: najprej plačilo, potem blago ali obratno.

4.1. PLAČILNE KARTICE

Plačilna sredstva na internetu so elektronske različice klasičnih plačilnih sredstev. Bistvena razlika je, da v elektronski različici vse poteka po elektronski poti in v nobeni fazi poslovanja ni fizične prisotnosti plačilnega sredstva.

Poznamo debetne, kreditne ter posojilne plačilne kartice. Najbolj razširjene so Visa, Mastercard/Eurocard, American Express ter Diners. Ko želimo v trgovini plačati s plačilno kartico, jo prodajalec vstavi v POS terminal, ki s čitalcem za magnetni zapis prebere podatke o lastniku

kartice. POS terminal se z vgrajenim modemom poveže s procesnim centrom, ki ugotovi izvor kartice. Če je kartica tuja, se podatki posredujejo v tujino, če kartica pripada izdajateljem, za katere procesni center obdeluje podatke, jih obdela center, če pa kartica pripada izdajateljem drugih procesnih centrov, se podatki posredujejo njim. Procesni center nato ugotovi, ali je transakcija dovoljena in s tem seznani POS terminal. Komunikacija pri tem postopku poteka po navadnih klicnih telefonskih linijah, ki se uporabljajo tudi za prenos govornih ali telefaks sporočil. Prodajalčeva dolžnost je, da s pomočjo podpisa prinesitelja kartice in podpisa na kartici preveri, če je prinesitelj zares lastnik kartice, saj večina kartic ni prenosljivih. Zaradi večje varnosti so se v trgovinah pojavili POS terminali, v katere prinesitelj kartice vtipka osebno geslo, ki ga za razliko od podpisa ni mogoče ponarediti in ga je praktično nemogoče ugotoviti brez dodatnih informacij.

Sistem SET[18]

Na internetu ni mogoče preveriti, če je oseba, ki kupuje blago ali storitev, res lastnik kartice, s katero namerava plačati. Zato je zelo pomembno, da svoje številke kreditne kartice ne pošiljamo nezaščitene po spletu. Najbolj znan sistem za elektronsko plačevanje s kreditno kartico je protokol za varno transakcijo ali SET. Ta protokol predvideva udeležbo treh strank: kupca, trgovca in vmesnega sistema oziroma banke, ki izpelje denarno transakcijo. SET zagotovi vmesna vrata med nezavarovanim delom interneta in varnim omrežjem bank, prek katerega se opravljajo elektronske denarne transakcije. Vse tri stranke v postopku so opremljene s parom asimetričnih ključev, zasebnim in javnim. Pari ključev se uporabljajo za avtorizacijo, preverjanje identitete, preprečitev zanikanja transakcije in zagotovitev tajnosti. Kupec pošlje informacijo o kreditni kartici na varni del omrežja skozi prodajalčev sistem, ki mu transakcijsko omrežje odgovori z avtorizacijo plačila.

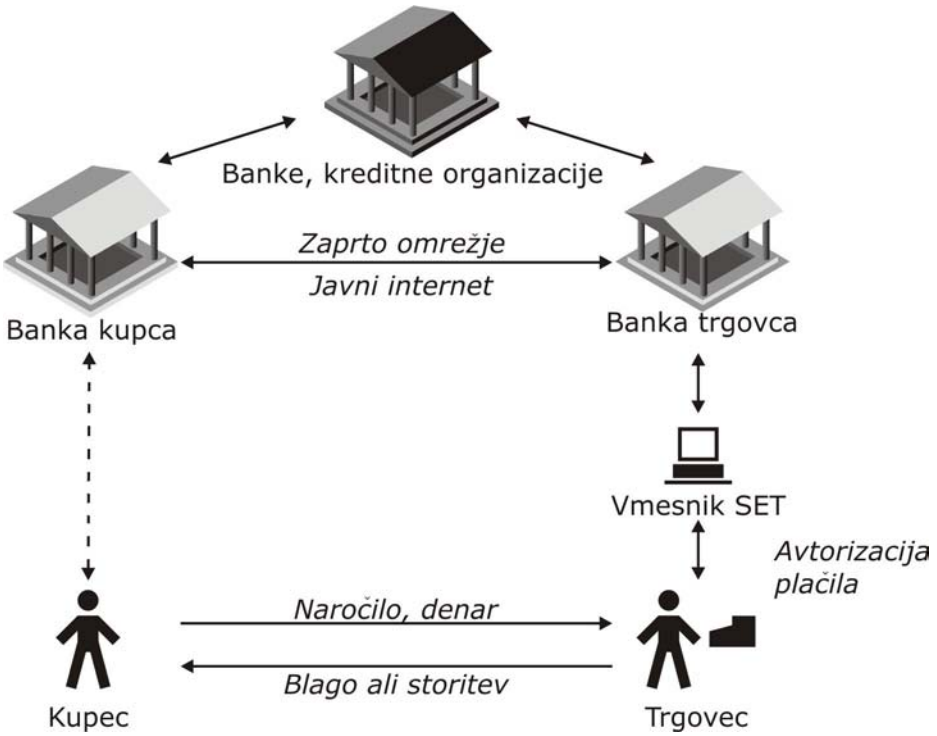
Identiteta kupca je delno zaščitena tako, da so podatki o nakupu in kupčevi kreditni kartici porazdeljeni med prodajalca in banko, ki opravi transakcijo. Delovanje sistema SET je prikazano v sliki 1.

Ko kupec izbere blago in kartico, s katero bo plačal (Master, Visa ali Eurocard), naročilo in način plačila podpiše s svojim zasebnim ključem in to pošlje prodajalcu. V naročilu je številka kreditne kartice, ki je

[18] *Secure Electronic Transaction*

zašifrirana tako, da jo lahko prebere le vmesni sistem. Informacije o kreditni kartici skupaj z vrednostjo naročenega blaga vmesniku SET pošlje prodajalčev sistem, ki te informacije podpiše s svojim zasebnim ključem. Vmesni sistem preveri veljavnost kreditne kartice, hkrati pa še identiteto trgovca. Po opravljeni avtorizaciji pošlje informacijo trgovcu, da je plačilo avtorizirano, ta pa sporoči kupcu, da sprejema plačilo. To sporočilo vmesni sistem digitalno podpiše. Kasneje bo prodajalec zahteval od vmesnega sistema prenos denarja na njegov račun. Avtorizacijo plačila za posamezni nakup se zahteva pri vsakem nakupu posebej, prenos denarja na trgovčev račun pa se opravi za več opravljenih avtorizacij v različnih časovnih obdobjih.

Slika 1: Sistem SET



Vir: Jerman-Blažič, 2001, str. 136.

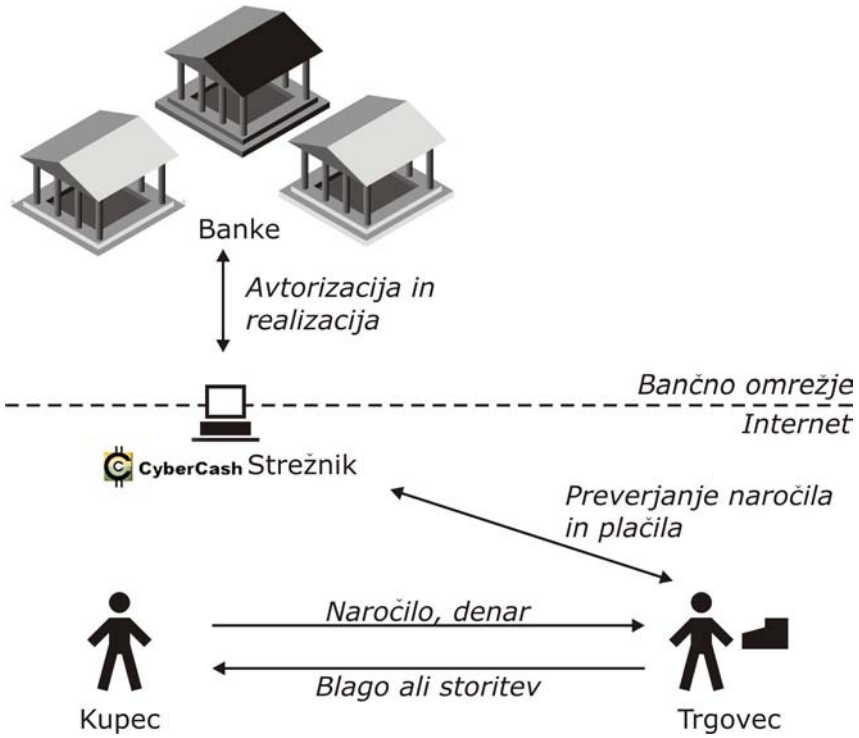
Identiteta kupca je delno skrita, ker trgovec lahko razbere le naročilo, ne pa tudi identitete kupca. Vmesni sistem dobi informacijo o identiteti kupca z informacijo o kreditni kartici, ne dobi pa podatkov o vsebini naročila, ker je ta informacija skrita s pomočjo tehnike, znane kot dvojni podpis. Kupec pošlje prodajalcu sporočilo, ki vsebuje dva dela: specifikacijo načina plačevanja, ki vsebuje identifikacijsko številko kupca in informacijo o kreditni kartici, ter drugi del, ki vsebuje informacijo o vsebini naročila. Ta dva dela sta dvojno podpisana tako, da je za vsakega izdelan ločen 'prstni odtis', 'prstna odtisa' pa sta podpisana skupaj. En sprejemnik dobi čistopis

prvega dela in 'prstni odtis' drugega dela, drug sprejemnik pa ravno obratno, 'prstni odtis' prvega dela in čistopis drugega dela. Oba 'prstna odtisa' sta skupaj povezana z zasebnim ključem kupca in sta neločljivo povezana. Tako lahko vsak sprejemnik preveri neokrnjenost podatkov celotnega sporočila, prebere pa le tisti del sporočila, ki mu je namenjen.
Kljub izjemni varnosti in podpori organizacij za izdajo kreditnih kartic (Visa, Mastercard) ter dobaviteljev opreme (IBM, Microsoft, Netscape) ni prišlo do množične uporabe standarda. Nekompatibilnost računalniške programske in strojne opreme ter kompleksnost sistema SET je omejila njegovo uporabo. Ideja, da bi ustvarili odprti sistem plačevanja s kreditno kartico preko javnega omrežja, tako nikoli ni do konca zaživela.

CyberCash
Podjetje CyberCash je bilo eno izmed prvih podjetij, ki je ponudilo varno elektronsko plačevanje prek interneta z različnimi kreditnimi karticami ali z uporabo bančnega računa. CyberCashov centralni strežnik se postavi v vlogo vmesnega sistema, ki mu kupci plačujejo s kreditnimi karticami. Po prejetju denarja od kupčeve banke CyberCash na klasičen način nakaže denar banki prodajalca in za to uslugo obdrži nekaj odstotkov. Pred uporabo sistema si mora kupec naložiti programsko opremo, ki jo prenese s strežnika CyberCash in ki mu omogoča generiranje parov ključev. Nato podpiše pogodbo, ki ureja pravice in odgovornosti kupca ter CyberCasha in vsebuje številko kreditne kartice ali bančnega računa kupca. Uporabnik digitalno podpiše in žašifrira pogodbo ter jo pošlje Cybercashu po internetu. Od tu naprej lahko uporabnik kupuje ali prodaja po internetu. Ko najde ugodno ponudbo in prodajalca, ki sprejema plačilo prek CyberCasha, prenese z mreže ponudbo prodajalca. Kupec potrdi, da sprejema prodajalčevo ponudbo tako, da digitalno podpiše ponudbo in doda svojo številko kreditne kartice, ki jo zašifrira s CyberCashejevim javnim ključem. To sporočilo prodajalec digitalno podpiše in ga pošlje CyberCashejevemu strežniku. Strežnik vzpostavi povezavo z ustrezno banko ali organizacijo, ki je izdajatelj kreditne kartice kupca, in sproži denarno transakcijo, če je kartica veljavna. Prodajalec dobi informacijo o opravljeni transakciji, kupec pa potrdilo od prodajalca o tem, da je bilo blago plačano. Delovanje sistema CyberCash je prikazano v sliki 2.

Podjetje CyberCash je pred kratkim prevzelo podjetje Verisign, eno od največjih podjetij, ki nudijo storitve za varno elektronsko poslovanje.

Slika 2: Sistem CyberCash



Vir: Jerman-Blažič, 2001, str. 139.

Protokol SSL

Protokol SSL se pogosto uporablja v elektronskem bančništvu. Uporabnik se najprej prepriča, ali komunicira s pravim bančnim strežnikom, hkrati pa lahko tudi strežnik preveri identiteto stranke. Po vzajemnem preverjanju SSL zagotovi neokrnjenost izmenjanih podatkov in zaupnost informacij. Protokol SSL je sestavljen iz dveh delov. *SSL Handshake protocol* omogoča usklajevanje algoritmov, overjanje strežnika in odjemalca, prenos digitalnih certifikatov in določitev skupnega ključa za simetrični kriptoalgoritem. Drugi del je *SSL Record protocol*, ki definira format izmenjanih podatkov in zagotavlja neokrnjenost ter šifriranje. Uporabo protokolov SSL in TLS v svetovnem spletu spoznamo po predponi *https* namesto *http*.

Prav tako se je SSL zaradi zapletenosti sistemov, ki uporabljajo storitve vmesnega sistema, uveljavil tudi za elektronsko plačevanje blaga in storitev na internetu. Z uporabo SSL sistema zagotovimo, da oseba, ki morda nadzira promet s trgovčevim računalnikom, ne pride do vsebine podatkov, saj se pri vzpostavitvi povezave med strežnikom prodajalca in kupčevim brskalnikom vzpostavi varen kanal, ki onemogoča prisluškovanje podatkom. Vendar pa to ne pomeni, da so prenešeni podatki varni pred zlorabo s strani trgovca, saj jih SSL zaščiti le med

prenosom med odjemalcem in strežnikom. Zato je izredno pomembno, da uporabnik zaupa trgovcu in se prepriča o njegovem poslovanju, preden se odloči za nakup preko spleta. Preveriti mora, ali je spletna trgovina označena z znakom, ki potrjuje, da je trgovina varna. Najbolj znano in uveljavljeno podjetje, ki skrbi za varnost spletnih trgovcev, je podjetje VeriSign. Dodatna pojasnila o varnem poslovanju si lahko kupec prebere na spletnih straneh vsake e-trgovine. Potrebno jih je skrbno prebrati in se tako še dodatno prepričati, kako spletni trgovec skrbi za varnost kupčevega in svojega poslovanja. Ko trgovec prejme podatke o kupčevi kartici, jih preko sistema, ki je povezan v varno bančno omrežje, preveri in če je kartica veljavna ter organizacija ali banka, ki jo je izdala, avtorizira plačilo, javi kupcu, da sprejme plačilo. Tako se lahko nakup izpelje do konca.

4.2. ELEKTRONSKO PLAČEVANJE S POMOČJO BANČNEGA RAČUNA

Podoben sistem kot je sistem CyberCash je leta 1994 predstavilo podjetje First Virtual, le da kupec tu ni uporabljal kreditne kartice, ampak obstoječi bančni račun. Kupec je plačal blago šele po prevzemu in je imel tako možnost zavrniti plačilo po dobavi blaga, če je imel za to utemeljene razloge. Nalog za denarno transakcijo je čakal na kupčevem računu pri First Virtual. V tem sistemu je imel kupec določeno prednost pred trgovcem. Leta 1998 je podjetje First Virtual prevzelo podjetje CyberCash in tako se je prenehala uporaba odloženih plačil z bančnih računov.

4.3. ELEKTRONSKI DENAR

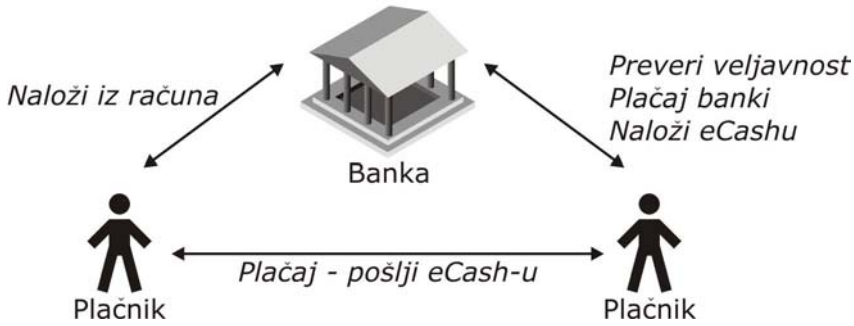
V večini elektronskih plačilnih sistemih morata tako kupec kot prodajalec dokazati svojo identiteto. Zato je David Chaum leta 1985 prišel na idejo o elektronskem denarju, ki bi kupcu zagotovila podobno anonimnost, kot mu jo klasično plačevanje z gotovino. Na drugi strani pa sodelovanje med kupcem in banko omogoča, da je identiteta prodajalca dokazljiva. Njegovo delovanje bomo prikazali na podlagi sistema eCash.

eCash

Preden uporabnik začne uporabljati eCash, potrebuje račun pri banki, ki podpira plačilni sistem eCash. Ko ima uporabnik račun, mu banka generira elektronske kovance in vsakemu posebej določi serijsko številko. Za začetek plačevanja uporabnik potrebuje še program za poslovanje eCash, ki ga prav tako dobi pri banki. Poleg programa dobi uporabnik še

identifikacijsko številko in ustrezno uporabniško geslo. Elektronske kovance kupec hrani v elektronski denarnici na lokalni delovni postaji. Pri nakupu kupec pošlje kovance prodajalcu po medmrežju, ta pa jih preveri pri banki, ki jih je izdala. Vsak kovanec se lahko uporabi le enkrat, banka pa kovance preverja po bazi porabljenih kovancev in jih ne sprejme, če se kovanci nahajajo v tej bazi. Na trgovčevem računu eCash se poveča stanje za vsoto prejetih kovancev, poleg tega pa se v bazo porabljenih kovancev vpišejo serijske številke kovancev, uporabljenih v transakciji. Delovanje sistema eCash je prikazano v sliki 3.

Slika 3: Sistem eCash



Vir: Jerman-Blažič, 2001, str. 141.

Podobno kot pri klasičnem plačevanju z gotovino sistem eCash omogoča polaganje in dvigovanje gotovine z bančnega računa. Poglavitna razlika med klasičnim in elektronskim plačevanjem z gotovino je, da si v elektronskem načinu kupec in prodajalec ne morete neposredno izmenjati denarja, saj je za transakcijo potrebna še tretja oseba, banka. Res pa je, da banka pri svojem posredovanju nikjer ni vidna in se zdi, da uporabniki med seboj brez posredništva pretakajo denar iz ene elektronske denarnice v drugo. Banka tako svojo pomembno vlogo odigra na diskreten način.

Prednost digitalnega denarja pred klasičnim je, da se lahko izdaja v poljubnih vrednostih. Elektronski denar je lahko nominiran v večjih ali manjših poljubnih vrednostih (123 SIT; 0.5 SIT; 5343.23 SIT). Tako je denominacija digitalnega denarja lahko precej manjša od vrednosti, ki jih poznamo v realnem življenju. Vendar pa obstaja transakcijski minimum, saj banke za vsako transakcijo zaračunajo uporabniku transakcijsko pristojbino. Če ne bi bilo transkakcijskega minimuma, bi se lahko zgodilo, da bi bila pristojbina večja od same vrednosti transakcije. To je le teoretičen problem, saj so v elektronskem poslovanju transakcijski stroški ponavadi zelo nizki. Zato so tudi bančne provizije zelo majhne in trgovci lahko prodajajo precej majhne 'kose' informacije (vremensko poročilo,

stanje neke delnice). Takšne majhne denominacije so imenovane mikrodenar, transakcije z mikrodenarjem pa mikrotransakcije.

Sistem eCash je februarja leta 2000 v Nemčiji uvedla Deutsche Bank, vendar se je storitev zelo počasi uveljavljala. Programska oprema je varna in zanesljiva, njena namestitev pa precej zahtevna. Poslovanje z eCashom je podprlo malo internetnih trgovin. Zato se danes ta sistem ne uporablja več.

4.4. ELEKTRONSKI ČEK

Navaden klasičen ček je pisni nalog kupčevi banki, da s kupčevega računa prenese določen znesek na račun prodajalca. Ček se izroči prodajalcu, ki ga posreduje banki, da se transakcija izvrši do konca. Po izvršenem prenosu ček ni več veljaven. Podobno vlogo ima tudi elektronski ček. Deluje kot sporočilo oziroma nalog za prenos sredstev in je izročen prodajalcu, ki ga kasneje izroči banki. Tako vrsto plačilnega sredstva je ponudil CyberCash kot dodatek k poslovanju s kreditnimi karticami. Postopek plačila je zelo podoben plačevanju s kreditno kartico, le da se CyberCashov strežnik tokrat ne pojavi kot posrednik pri transakciji, ampak to vlogo opravijo banke. Uporabnik dobi elektronski račun, s katerim posluje.

Obstaja pa tudi sistem, ki za poslovanje zahteva elektronski naslov, čitalnik pametnih kartic in račun pri banki, ki podpira sistem za poslovanje z elektronskimi čeki. Razvili so ga pri FSTC, konzorciju bank in klirinških hiš. Njihov elektronski ček je podoben klasičnemu, le da so mu dodali elektronski podpis.

4.5. SISTEMI AKTIVNIH PLAČILNIH KARTIC

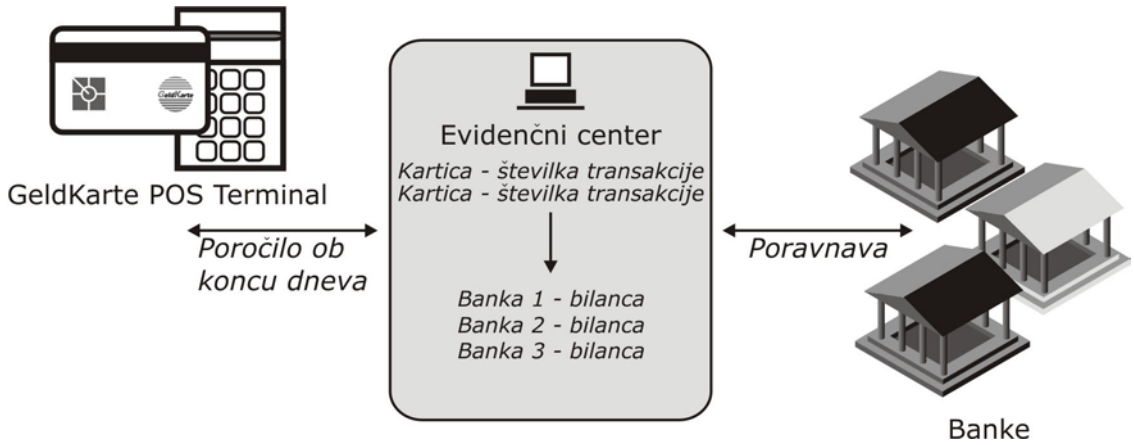
Mondex
Sistem Mondex se je začel razvijati že leta 1990. Mondex uporablja tako pametno kartico kot elektronsko denarnico in je definiran kot protokol med čipi, ki so instalirani na prodajnih mestih, v osebnih terminalih, napravah kupcev, v elektronskih denarnicah ali v pasivnih karticah. Medij za prenos je lahko internet, telefonska povezava ali lokalni čitalnik kartic v terminalih Mondex in Mondexovih denarnicah. Vsak lastnik kartice lahko izmenjuje denar s katerokoli denarnico drugega lastnika. Denarnica Mondex vzdržuje stanje kovancev oziroma denarja v petih različnih

valutah. Sistem Mondex ne zagotavlja anonimnosti, saj banka Mondex spremlja vse podatke o vsaki transakciji in tako spremlja pretok denarja tako na kupčevem kot na prodajalčevem računu. Sistem Mondex je od julija 2001 v lasti podjetja MasterCard International in je najbolj razširjen sistem za plačevanje z aktivnimi plačilnimi karticami, saj se uporablja na vseh kontinentih. Z njim je moč poslovati preko digitalne televizije (TV prodaja, elektronsko bančništvo), preko interneta (igre na srečo) ter preko mobilnega telefona.

GeldKarte

Najbolj razširjen sistem na osnovi pametnih kartic v Nemčiji je sistem GeldKarte[19]. Zasnovan je na čipu, ki je lahko postavljen na navadni kreditni kartici ali pa na posebni "beli kartici", ki ni povezana z bančnim računom. Slednje zagotavlja anonimno plačevanje, napolni pa se lahko le z gotovino na terminalu. Pri beli kartici lahko uporabnik napolni svojo kartico GeldKarte na bančnem terminalu s prenosom sredstev s svojega bančnega računa. Za vsako transakcijo doda prodajalec zapis o njej v svoj lokalni račun GeldKarte. V zapisu je navedena količina in ustrezni bančni račun. Če je kartica GeldKarte vezana na kreditno kartico, potem je to bančni račun lastnika kartice, v primeru bele kartice pa je to skupni račun vseh belih kartic banke izdajatelja. Po koncu poslovanja prodajalec pošlje informacije o dnevnem izkupičku na svojem lokalnem računu GeldKarte vmesnemu sistemu, ki skrbi za poravnavo in prenos denarja med bankami. Delovanje sistema GeldKarte je prikazano v sliki 4.

Slika 4: Sistem GeldKarte



Vir: Jerman-Blažič, 2001, str. 148.

[19] *denarna kartica*

Banke poznajo povezave med kartico in njenim lastnikom, vmesni sistemi pa med kartico in posameznim nakupom. Tako se v primeru nuje ali zlorabe lahko razkrije kupec, vendar to ni možno v primeru bele kartice.

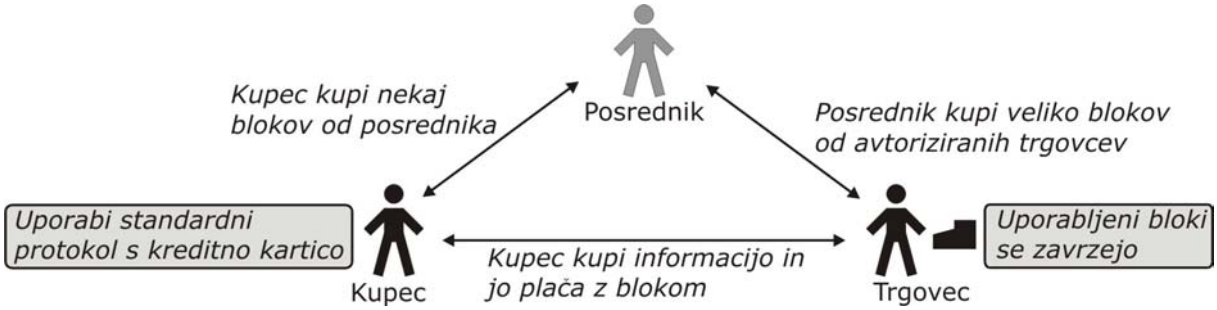
Žal pa ima večina sistemov pametnih kartic podoben problem in sicer slabo sprejetje s strani trgovcev ter nekompatibilnost med karticami in elektronskimi denarnicami različnih sistemov.

4.6. SISTEMI ZA MIKROPLAČILA

Zaradi sistemov za digitalno podpisovanje in šifriranje s pomočjo javnih ključev ter metod za prepričevanje zanikanja vsaka transakcija povzroči določene stroške. Za plačevanje zelo nizkih zneskov so se tako razvili sistemi za mikroplačila. Ti sistemi vključujejo postopke, ki zagotavljajo manjše stroške za varnost in komunikacijo.

Eden izmed prvih sistemov za mikroplačila je bil sistem *Milicent*. Protokol vključuje kupca, prodajalca ter posrednika. Posredniki kupijo od prodajalca veliko blokov z določeno vrednostjo in jih potem prodajajo kupcem po kosih, ki imajo po navadi vrednost od enega do deset EUR. Bloki so dejansko elektronski denar, ki se izda le enkrat in se lahko uporablja večkrat do porabe njegove nominalne vrednosti. Prodajalec sprejme blok le, če ima ta nominalno vrednost in kupcu vrne razliko, če je vrednost nakupa manjša od vrednosti bloka. Delovanje sistema Milicent je prikazano v sliki 5.

Slika 5: Sistem Milicent



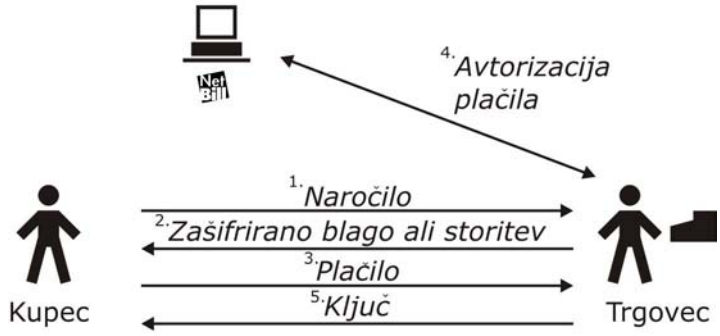
Vir: Jerman-Blažič, 2001, str. 150.

Kupci v sistemu Milicent so po navadi dolgoletne stranke posrednikov, pri katerih poravnavajo račune elektronsko ali na klasičen način. Zaradi varčevanja pri stroških komunikacije se pri plačevanju veljavnost bloka ali identiteta kupca ne preverja. Bloki imajo določene lastnosti, ki omogočajo

takojšnjo ugotovitev ali so lažni ali pravi, poleg tega pa je zaradi njihove nizke vrednosti verjetnost poneverjanja razmeroma nizka. Sistem Milicent se zato šteje za varnega.

Podoben sistem je razvijal tudi IBM, ki ga je poimenoval MiniPay. Kljub temu, da sta oba sistema zaživela na internetu, se njuna uporaba ni razširila. Podobno se je godilo tudi sistemu *NetBill*, ki sta ga razvili podjetje Visa International in Carnegie Mellon University in ga je kasneje v svoj sistem pripojil CyberCash. Sistem NetBill je sistem za mikroplačila, razvit posebej za plačevanje elektronskih produktov in storitev na internetu. Sodelujoči stranki v poslu morata imeti instalirano NetBill programsko opremo Money Tool. Ko kupec izbere želeni produkt, mu ga trgovec pošlje, vendar zašifriranega, tako da ga kupec še ne more uporabljati. Ko trgovec prejme denar iz vnaprej napolnjenega kupčevega NetBill računa, pošlje kupcu ključ za dešifriranje produkta. S tem so v sistemu NetBill onemogočili možnost zlorabe. Potek transakcij v sistemu NetBill je prikazan v sliki 6.

Slika 6: Sistem Netbill



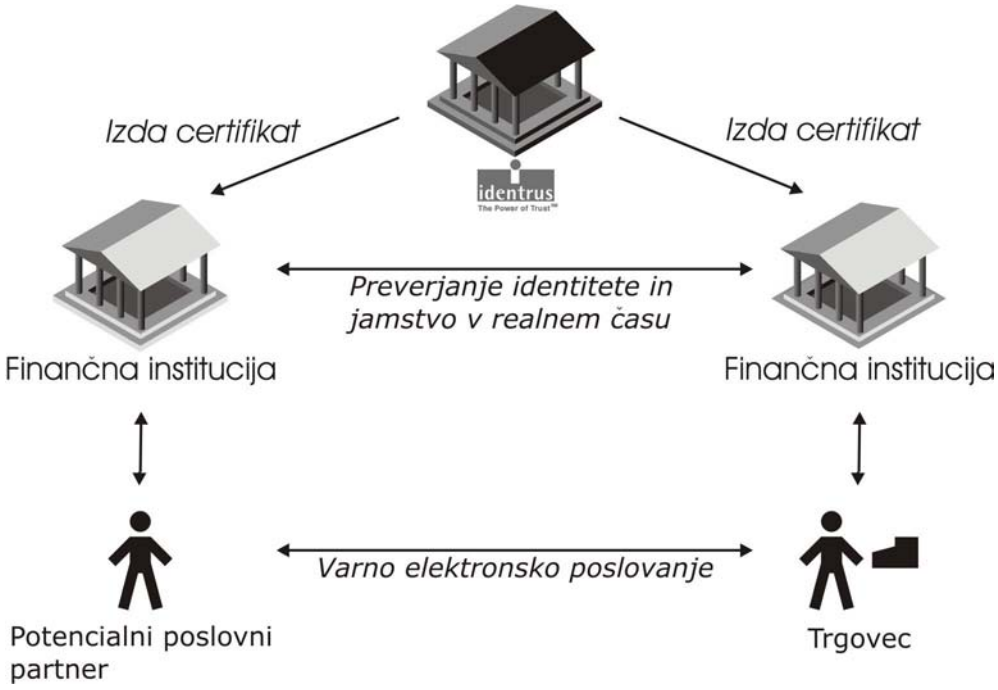
Vir: Stolpmann, 1997, str. 77.

4.7. SISTEM VARNEGA PLAČEVANJA MED PODJETJI

Do sedaj sem predstavil sisteme za elektronsko plačevanje med podjetji in njihovimi strankami. Večina teh sistemov ni primerna za elektronsko poslovanje med podjetji. Zato je skupina bank (ABN AMRO, Bank of America, Bankers Trust, Barclays, Chase Manhattan, Citigroup, Deutsche Bank and Hypo Vereinsbank) v aprilu leta 1999 ustanovila podjetje *Identrus*. Sistem omogoča podjetjem konsistenten poslovni proces, globalen pristop, uporabo standardov odprtih sistemov, jasno pravno varnost in oceno tveganja pri elektronskem poslovanju. Identrus je zasnovan na hierarhični infrastrukturi javnih ključev, pri čemer Identrus na vrhu predstavlja skupno točko zaupanja med sodelujočimi. Naslednjo

raven predstavljajo sodelujoče banke (danes jih je že prek 50), tretja raven pa vsebuje manjše finančne institucije in korporacije, ki izvajajo elektronsko poslovanje med podjetji zase in za manjša podjetja, s katerimi imajo sklenjene sporazume. Delovanje sistema Identrus je prikazano v sliki 7.

Slika 7: Sistem Identrus



*Vir: (*URL:http://www.identrus.com/knowledge/pubs/Overview_Brochure.pdf), 2002).

Prenos denarja poteka po klasičnih, znanih poteh, ki jih banke obvladajo že desetletja. Najmočnejša lastnost sistema Identrus je v infrastrukturi javnih ključev, ki mu omogoča izpeljavo vseh poslov, vezanih na prenos denarja (plačevanje, zavarovanje, sklenitev pogodb).

Telekomunikacijske in informacijske tehnologije doživljajo veliko rast. Skupaj krojijo prihodnost. Mobilno poslovanje in mobilni dostop do interneta ustvarjata nove izzive poslovanja podjetij vseh panog, internet sam pa beleži dinamično rast – tako na področju uporabe kot tudi izrabe njegovih prednosti. Čeprav se iz dneva v dan širi, pa sistemi za elektronska plačila ostajajo bolj ali manj nespremenjeni. Razvoj elektronskih plačilnih sistemov se je preselil v mobilno omrežje, ki s pojavom sistema GSM nudi vedno več glasovno in podatkovno orientiranih storitev.

Skupina GSM je bila ustanovljena leta 1985 z namenom združiti mobilne telefonske sisteme, ki so do tedaj bili nekompatibilni in so bili osnovani na analognih radijskih komunikacijah, ki niso zadovoljile nikakršnih varnostnih zahtev. Tako je bilo že od začetka jasno, da bo uporabljena digitalna tehnologija, ki bo zagotavljala večjo kvaliteto prenosa govora in simultano prenašanje večjega števila pogovorov po omejenem frekvenčnem pasu. Kasneje, z razvojem omrežja in mobilnih terminalov, pa je prišlo še do nove možnosti uporabe mobilnih telefonov in sicer prenos podatkov.

Za prenos podatkov se danes uporabljata 2 sistema: CSD[20] in GPRS[21]. Prvi sistem omogoča večjo konstantnost prenosa, drugi pa navidezno dosega višje hitrosti. S pomočjo teh dveh sistemov so nam trenutno na voljo naslednje podatkovne storitve:

- WAP – *Wireless Aplication Protocol* – nam omogoča pregledovanje spletnih strani, prirejenih za mobilne telefone;
- JAVA – je objektno orientiran programski jezik, ki ga je razvilo podjetje SUN Mycrosystems, s katerim je moč izdelovati uporabne programe in igrice;
- SMS – *Short Message System* – sporočilo, ki lahko vsebuje do 160 alfanumeričnih znakov latinice in 70 znakov nelatinskih pisav;
- MMS – *Multimedia Message System* - nova storitev, ki se pojavlja na trgu, ki poleg teksta omogoča tudi pošiljanje slik.

V trenutni ponudbi storitev mobilne telefonije še ni plačljivih storitev, ki se obetajo v tretji generaciji mobilne telefonije, imenovani UMTS[22,] kot na primer video na zahtevo, video v realnem času in podobno. Pa vendar v svetu že razvijajo sisteme, ki omogočajo plačevanje najrazličnejših storitev z mobilnim telefonom.

4.8. PLAČEVANJE Z MOBILNIM TELEFONOM

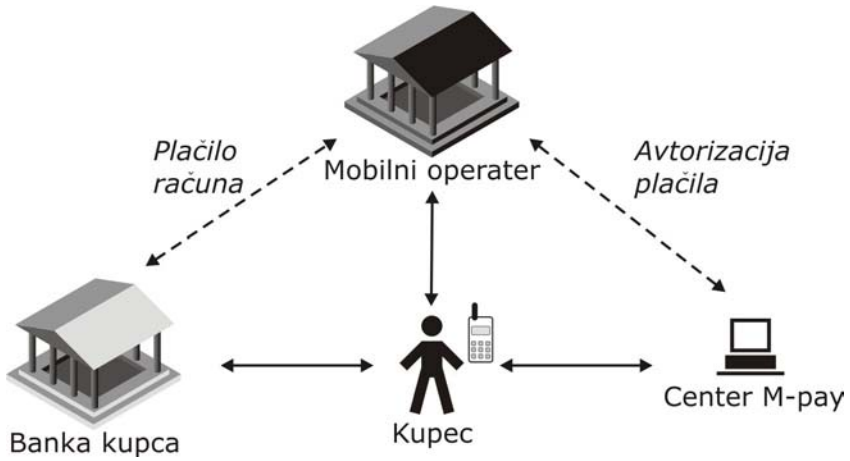
Sistemi za plačevanje s pomočjo mobilnega telefona so še v razvoju, saj se tudi mobilna telefonija še razvija. V svetu se testno uveljavlja tretja generacija mobilne telefonije, medtem ko v Sloveniji le-to še pričakujemo. Kljub temu pa že poznamo sisteme za plačevanje preko mobilnih telefonov. Eden takih je tudi sistem M-pay podjetja Ultra d.o.o.

[20] *Circuit Switched Data*
[21] *General Packet Radio Service*
[22] *Univerzalni Mobilni Telekomunikacijski Sistem*

M-pay

Osnovni princip delovanja terminala M-Pay je prenos podatkov v center M-Pay in nazaj v obliki zvoka. Terminal M-Pay prenese identifikacijo prodajnega avtomata ter znesek plačila v center M-Pay preko zveze, ki jo je vzpostavil kupec s svojim mobilnim telefonom. V centru na podlagi podatkov o kupcu (kupec se identificira s pomočjo funkcije CLIP) preverijo zmožnost kupčevega plačila (ali je kupec že registriran kot uporabnik sistema M-PAY sistema, koliko sredstev ima na računu, itd.) ter nato odobrijo sam nakup in izvedejo transakcijo s kupčevega računa. Sodelujoči subjekti v sistemu M-pay so prikazani v sliki 8.

Slika 8: Sistem M-pay



Vir: (URL:http://www.m-pay.com/dsg/overview.pdf), 2002).

Dejansko plačilo v sistemu M-Pay se opravi z enako lahkoto kot telefoniranje: uporabnik pokliče avtorizacijski center, ki ugotovi številko njegovega telefona. Nato prisloni mobilni telefon k plačilnemu terminalu M-Pay ter počaka, da se prenos zaključi. Če je višina zneska transakcije v okviru uporabnikovega limita oziroma stanja na predplačniškem računu, avtorizacijski center nakup odobri. Znesek nakupa se pripiše na uporabnikov račun za telefon in se poravna hkrati z drugimi mobilnimi storitvami, pri predplačniških uporabnikih pa se stanje na računu zmanjša takoj.

V plačilnem sistemu M-Pay je za varnost poskrbljeno na več nivojih. Uporabnikova identiteta je enolično določena na podlagi SIM kartice v mobilnem telefonu. Pristnost plačilnega terminala in plačilnega centra se preveri z digitalnim podpisom na osnovi kriptografskega sistema ECC[23].

[23] *Elliptic Curve Cryptography*

Uspešen digitalni podpis je osnova za šifriranje transakcije. Na ta način so zavarovane vse stranke v sistemu: kupci, trgovci in plačilni center.

5. STANJE ELEKTRONSKIH PLAČILNIH SISTEMOV V SLOVENIJI

5.1. PLAČILNE KARTICE

V Sloveniji smo na področju debetnih, kreditnih in posojilnih kartic v koraku s časom. Najbolj so pri nas uveljavljene kartice z odloženim plačilom, pri katerih se obveznosti plačujejo enkrat na mesec. Te kartice so: domači Karanta in Activa ter najbolj razširjeni tuji kartici Eurocard/Mastercard in Visa. Vse večje banke v Sloveniji ponujajo vsaj eno izmed teh kartic na podlagi odprtega tekočega računa. Za vsako kreditno kartico je treba plačati letno članarino, ki pa se razlikuje glede na vrsto kartice (navadna, poslovna, zlata) in banko. Te kartice so namenjene predvsem plačevanju, zato je za dvigovanje gotovine na bankomatu ali v banki treba plačati razmeroma visoko provizijo.

Najnovejše plačilne kartice, ki so se pojavile v Sloveniji, so debetne kartice in jih je tudi največ. Njihova značilnost je, da omogočajo takojšno obremenitev računa imetnika in deloma zamenjujejo gotovinsko plačevanje. To so kartice tekočih računov, ki jih uporabljamo tudi za dvigovanje gotovine na bankomatih in imajo oznako Cirrus Maestro ali Visa Electronic. V zadnjem času je moč s temi karticami plačevati tudi v tujini, v trgovinah z oznako Maestro ali Visa Electronic.

Poleg bančnih kartic poznamo tudi podjetniške kartice. Najstarejša mednarodna plačilna kartica, ki je v Sloveniji prisotna že dvajset let, je Diners Club, ki je v Sloveniji za partnerstvo pridobil veliko večjih slovenskih podjetji (Nama, Adria Airways, Merkur, Mobitel, Generali, Delo, Slovenske železnice). Poleg Diners Cluba pa je v Sloveniji še nekaj domačih podjetniških plačilnih kartic. Prvo podjetje je bil Petrol, ki je izdal kartico Magna za plačevanje na Petrolovih bencinskih črpalkah. Svojo kartico je izdalo tudi podjetje Istrabenz. Mercator pa je ponudil prvo pametno kartico, ki na čip zapisuje število točk, ki se kasneje uporabljajo za določene ugodnosti.

5.2. INTERNET

V Slovenijo je internet prišel preko Inštituta Jožefa Stefana v okviru Laboratorija za odprte sisteme in mreže ter projekta YUNET. Leta 1993 sta Mark Martinec in Žiga Turk s FAGG[24] začela razvijati WWW strežnike v Sloveniji. Strežnik, ki ga je postavil Mark Martinec je bil sprva mišljen kot predstavitvena stran Inštituta in z nekaj splošnimi informacijami tudi predstavitvena stran Slovenije. Postavitev WWW strežnika je spodbudila mnoge akademske centre, da so razvili svoje predstavitve. Na otvoritveni strani se je tako oblikoval nekaj vrstični seznam WWW virov v Sloveniji.

Po podatkih Statističnega urada Republike Slovenije je v letu 2001 internet uporabljalo triindvajset odstotkov prebivalstva (Statistični letopis RS 2002, str. 380). Od tega jih je dvanajst odstotkov (Statistični letopis RS 2002, str. 380) opravljalo elektronske nakupe. Letopis sicer ne navaja, kje so bili ti nakupi opravljeni, v tujini ali v Sloveniji. Verjetno vsi nakupi niso bili opravljeni doma kljub temu, da imamo v Sloveniji kar nekaj internetnih trgovin. Podjetji EON in SiOL sta ustvarili vsak svoje spletno nakupovalno središče, v katerih sodeluje že preko petdeset najrazličnejših trgovin. Ti dve podjetji sta tudi ponudnika storitev za varno elektronsko plačevanje.

EON
Podjetje EON d.o.o. je bilo ustanovljeno leta 2000 in je bilo prvo podjetje v Sloveniji, ki je omogočalo on-line plačevanje v realnem času. Danes je EON tako imenovani CSP[25]. To pomeni, da zagotavlja infrastrukturo za spletno poslovanje. Infrastruktura je v tem primeru predvsem varna povezava med trgovcem, kupcem in finančnimi institucijami.

Varnost zagotavlja licenčni sistem Transact 4 ameriškega podjetja Open Market. Poleg varnega poslovanja omogoča sistem Transact 4 še vrsto drugih možnosti, predvsem s področja odnosov s strankami (ugotavljanje profilov kupcev, statistike nakupov, itd.), saj je moč s to programsko opremo vzdrževati register kupcev, torej vse tisto, kar potrebuje management trgovskega podjetja pri prilagajanju svoje ponudbe kupcem in s tem povpraševanju na trgu. Varnost pri prenosu naročila v internetnih trgovinah pod okriljem EON-a je zagotovljena z uporabo globalnega 128 bitnega digitalnega certifikata Verisign.

[24] *Fakulteta za arhitekturo, gradbeništvo in geodezijo*
[25] *Commerce Service Provider*

Postavitev sistema za varno internetno plačevanje stane podjetje, ki se za to odloči pri EON-u, dvajset tisoč SIT za priklop in petdeset tisoč SIT letne naročnine. Prav tako EON kot transakcijski strošek obdrži 1.5 do 3 odstotke plačila blaga ali storitve. Sistem lahko podjetje implementira v svojo spletno stran, lahko pa tudi v stran vstavi le gumbe za povezavo na EON-ov strežnik, kjer se izvrši transakcija.

EON-ov sistem za varno elektronsko plačevanje kot plačilno sredstvo sprejema skoraj izključno samo plačilne kartice. Nekatere trgovine in oddelki sprejemajo tudi naročilnice podjetij, s katerimi imajo sklenjeno pogodbo, ali pa čeke (po pošti). Katere kartice bo sprejemala internetna trgovina, je odvisno od tega, s katero banko podjetje, ki ima spletno trgovino, sodeluje in kakšne plačilne kartice banka izdaja.

SiOL
Tudi podjetje SiOL ponuja storitev varnega plačevanja po internetu s programsko opremo Transact Store. Svoje spletno nakupovalno središče so pri SiOL-u poimenovali eSiOL. Če se kupec odloči, da se bo registriral v ta sistem, to naredi s tako imenovano eDenarnico, ki služi SiOL-u za register kupcev. SiOL-ova eDenarnica je v SIOL-u implementiran elektronski plačilni sistem, ki omogoča varnejše, hitrejše in enostavnejše nakupovanje na spletu. Osebne podatke kupca in podatke o plačilnih sredstvih kupec v eDenarnico vpiše le enkrat, potem se ti varno shranijo na transakcijskih strežnikih SiOL-a in so dostopni le z vpisom kupčevega uporabniškega imena in gesla. Pri vsakem nadaljnjem nakupu kupcu podatkov ni potrebno ponovno vpisovati – za nakup izdelka zadošča le en klik.

5.3. MOBILNO OMREŽJE

Razvoj mobilne telefonije na slovenskem se je začel s pojavom NMT[26] omrežja leta 1991. Mobitel je prvo NMT centralo postavil leto kasneje. NMT sistem je bil prva generacija mobilne telefonije, ki je deloval še na analogni tehnologiji. Razvoj je šel v smeri digitalne tehnologije, druge generacije mobilne telefonije GSM. V Sloveniji je bilo pilotsko omrežje GSM postavljeno leta 1995, leto kasneje pa je podjetje Mobitel dobilo koncesijo za postavitev GSM omrežja. Dve leti kasneje je to koncesijo prejelo še podjetje Si-mobil in tako postalo konkurenčo podjetju Mobitel. V

[26] *Nordic Mobile Telephony*

letu 2001 je podjetje Mobitel imelo več kot milijon uporabnikov, kar je predstavljalo več kot polovico slovenskega prebivalstva. V tem letu se je pojavil še tretji operater, in sicer Vega.

Podjetju Mobitel se precej pozna dvoletni monopol, saj si je pred tekmeci s številom uporabnikov pridobil precejšnjo prednost. Tako je edini zmogel ugoditi pogojem za pridobitev licence za tretjo generacijo mobilne telefonije, UMTS, ki jo je pridobil v letu 2001. UMTS se bo pri nas pojavil v letu 2003, tako kot drugod v Evropi. Sistema nista izključujoča, tako da bo tudi sistem GSM ostal. Sistem UMTS je zelo podoben kabelskemu internetu, kjer je uporabnik stalno priključen na internet. Tako bodo tudi UMTS uporabniki stalno priključeni na omrežje in bodo lahko izkoriščali vse storitve mobilnega interneta: *multimedijo*, *videotelefonijo, poslušanje internetnega radia in ostalih glasbenih datotek, prenašanje datotek z visokimi hitrostmi (144 kbit na sekundo za hitro premikajoče terminale in 384 kbit na sekundo za počasno premikajoče terminale), s pomočjo GPS*[27] *sistema bo moč relativno natančno določiti mesto terminala* in tako naprej.

Po podatkih Statističnega urada Republike Slovenije je bilo v letu 2001 v Sloveniji že 75.8 odstotkov prebivalstva uporabnikov mobilne telefonije (Statistični letopis RS 2002, str. 380). Trend pospešenega naraščanja uporabnikov storitev mobilne telefonije je še posebej opažen po letu 1998, saj se je v treh letih število uporabnikov povečalo za skoraj šestkrat. V Sloveniji imamo štiri ponudnike storitev mobilne telefonije, poleg omenjenih še Debitel, ki pa nima lastnega omrežja, pač pa zakuplja Mobitelovo.

6. PLAČILNI SISTEMI V MOBILNEM OMREŽJU V SLOVENIJI

6.1. SISTEM MOBA

Podjetje Mobitel uvaja med svoje storitve vedno več storitev, povezanih z brezgotovinskim plačevanjem in mobilnim bančništvom. Tako je pred kratkim uvedel pametne SIM kartice, ki omogočajo, da preko mobilnega telefona uporabnik lahko pregleduje stanje tekočega računa oz. osebnega

[27] *Global Positioning System*

računa ali računa, za katerega je uporabnik storitve M-bančništvo pooblaščen.

Varnost je zagotovljena z ustreznim šifriranjem podatkov med uporabnikom in banko ter bančno PIN kodo (B-PIN). M-bančništvo je že na voljo vsem komitentom Nove Ljubljanske banke in bank bančne skupine Nove Ljubljanske banke, ki to storitev imenuje Moba.

6.1.1. PREGLED STORITEV

Sistem Moba nudi naslednje storitve:

- vpogled v stanje tekočega računa ali računa, na katerem je uporabnik pooblaščen;
- vpogled v promet na računu (zadnje štiri transakcije)
- vpogled v promet na računu, izveden prek mobilnega telefona (zadnje štiri transakcije);
- plačilo obveznosti prek plačilnega naloga in v prihodnje tudi plačilo nakupov v spletnih trgovinah;
- prenos sredstev med računi znotraj bančne skupine NLB;
- nastavitev alarmov o prekoračitvi osebnega limita
- naročilo povišanja limita na računu;
- vezavo sredstev;
- prijavo novega delovnega računa oziroma odjavo delovnega računa ter
- spremembo nastavitev (spremembo bančnega PIN-a ali spremembo naziva računa).

6.1.2. KAKO POSTATI UPORABNIK MOBE

Storitve Mobe NLB lahko uporablja imetnik ali pooblaščenec na tekočem računu, odprtem v Novi Ljubljanski banki oz. bankah bančne skupine NLB, ki je hkrati uporabnik omrežja Mobitel GSM (naročnik omrežja Mobitel GSM oziroma uporabnik predplačnega sistema Mobi ali naročnik Debitela). Za uporabo storitev potrebuje mobilni telefon z ustrezno pametno kartico SIM (mobilnega operaterja Mobitel ali ponudnika storitev Debitel) hkrati pa mora imeti pri mobilnem operaterju vključeno možnost uporabe storitev.

Pametno kartico je moč kupiti v Mobitelovem centru, Debitelu in pri izbranih Debitelovih pooblaščenih zastopnikih. Delovanje pametne kartice

podpira večina novejših modelov mobilnih telefonov. Prek Mobe NLB je moč poslovati tudi, kadar je uporabnik v tujini na območju pokritosti z GSM signalom Mobitelovih roaming partnerjev. Uporabniki predplačnega sistema Mobi si morajo za uporabo storitev v tujini pri mobilnem operaterju pred tem zagotoviti možnost pošiljanja sporočil SMS.

Na podlagi odobrene vloge za uporabo Mobe NLB naročnik prejme uporabniško številko in bančno osebno identifikacijsko številko (bančni PIN), ki ju potrebuje ob prijavi in uporabi storitev Mobe NLB na mobilnem telefonu. Uporabniško številko prejme ob prijavi za uporabo storitev v bančni poslovalnici ali prek Klika NLB. Bančni PIN pa mu banka pošlje po pošti. Tako je poskrbljeno za še večjo varnost, saj uporabniška številka in PIN ne potujeta po isti poti in ju je praktično nemogoče zlorabiti.

6.1.3. VARNOST V SISTEMU MOBA

Za varnost poslovanja prek Mobe NLB so poskrbeli z najsodobnejšimi varnostnimi tehnologijami, hkrati pa so omogočili dovolj udobno vsakodnevno uporabo.

Vsa sporočila SMS, ki si jih izmenjujeta uporabnik in banka, so šifrirana tako, da jih morebitni prisluškovalci ne morejo dešifrirati. Vsaka kartica SIM mobilnega telefona, ki je prijavljena za uporabo storitev mobilne banke, je enolično določena in za komunikacijo z banko uporablja svoj neponovljivi šifrirni ključ. Za vsak posamezni dostop do banke prek mobilnega telefona se oblikuje nov ključ, tako da ga nihče ne more uporabiti še enkrat, ko uporabnik konča delo.
Pri prijavi banke na mobilnem telefonu se mora uporabnik identificirati z unikatno določeno uporabniško številko in osebno dodeljenim bančnim PIN-om. Bančni PIN služi tudi za identifikacijo uporabnika pri opravljanju transakcij prek Mobe NLB, podobno udobno in varno kot pri poslovanju prek bančnega avtomata.

6.1.4. STROŠKI POSLOVANJA PREK MOBE

Stroški poslovanja prek Mobe NLB so odvisni od vrste opravljene storitve in trenutno znašajo:

- 10 SIT za vpogled v stanje računa,
- 20 SIT za vpogled v promet računa,
- 50 SIT za plačilo položnic in računov,

- 30 SIT za prenos sredstev med računi,
- 50 SIT za posredovano informacijo o prekoračitvi osebnega limita.

Ob prijavi uporabe storitev Mobe NLB banka zaračuna stroške enkratne pristopnine, ki danes znašajo 1.500 SIT oz. 750 SIT za dijake in študente. Stroške telekomunikacijskih storitev zaračunava mobilni operater na podlagi poslanih in prejetih varnih sporočil SMS v skladu z veljavnim cenikom za to storitev.

V letu 2001 je Mobitel prvič predstavil storitev Moneta, ki omogoča plačevanja majhnih zneskov na internetu, ter ga kasneje razširil še na sistem za plačevanje na raznovrstnih prodajnih avtomatih, v prihodnosti pa bo omogočala brezgotovinski nakup na prodajnih mestih, opremljenih s POS terminalom.

6.2. SISTEM MONETA

V primeru mobilnega interneta prihaja do težav predvsem na področju plačila. Skušajo zagotoviti čim boljšo varnost ter predstavlja nove, uporabnikom prijazne načine plačila. Prvi izmed slovenskih sistemov, ki rešuje dosedanje pomanjkljivosti načinov plačevanja na internetu, je Mobitelova storitev Moneta. To je storitev, ki si je na ljubljanskem sejmu Infos 2001 z izvirnostjo in tehnološko dovršenostjo zaslužila tudi naslov 'Najboljši na Infosu'.

Do sedaj sem predstavil elektronska plačilna sredstva, ki se ali pa so se uporabljala na internetu. Skupno vsem tem sistemom je, da imajo nekaj slabosti:

- med seboj niso povezani in od kupca zahtevajo, da pri vsakem prodajalcu izvede ločeno identifikacijo,
- kupec ima zaradi plačevanja pri različnih prodajalcih več uporabniških imen, PPC kod in drugih oblik identifikacije, kar je zamudno in neprimerno za nakupovanje manjših zneskov,
- sistemi od prodajalca zahtevajo prilagoditev programske opreme in obširne posege v aplikacijo,
- finančni vložki so poleg prodajalca pri vgraditvi ustrezne programske opreme lahko tudi na strani kupca.

Zahteva po enotni ureditvi, ki bo uporabnikom zagotovila univerzalen, enostaven, transparenten, čim manj moteč in fleksibilen sistem

plačevanja, ponudnikom pa prav tak sistem zaračunavanja storitev, izdelkov in informacij, je bila torej očitna. Zato je družba Mobitel v sodelovanju s podjetjema Adacta in Pristop d.o.o. razvila sistem plačevanja majhnih zneskov na internetu, ki odgovarja vsem tem zahtevam. To je sistem eMoneta. S sistemom M-pay so v avgustu 2002 testno uvedli še sistema aMoneta za plačevanje blaga in storitev na avtomatih ter posMoneto za plačevanje blaga in storitev preko POS terminala.

Moneta zagotavlja enostavno uporabo ter hitro izvedbo nakupa vsem Mobitelovim naročnikom GSM. Teh je danes že več kot 400.000, kmalu pa bo Moneta na voljo tudi skoraj 700.000 uporabnikom sistema Mobi. Uporabniku zagotavlja enoten in varen postopek identifikacije pri vseh ponudnikih blaga in storitev, ki so uvedli Moneto, ter ustaljen in enostaven potek plačila, pri čemer kupec plača le želene in zahtevane vsebine oz. blago. Moneta od ponudnika vsebin ali blaga na internetu ne zahteva dodatnih investicij v programsko opremo. Za uvedbo sistema je potrebno le preimenovanje naslovov hiperpovezav ali preimenovanje naslova strežnika.

6.2.1. KAKO DELUJE MONETA

Moneta omogoča tri oblike nakupov: običajen nakup, nakup s potrditvijo in naročilo. V vseh primerih je postopek za uporabnika enak, razlike nastajajo le na strani ponudnika.

Nakup
Moneta je primerna za prodajo vsebin in storitev majhnih finančnih vrednosti, najbolj uporabljana in hkrati priporočena pa je prodaja informacij. Moneta namreč omogoča hiter in povsem enostaven prehod iz neplačljivih v plačljive informacije. Če so se doslej nekatere informacije na spletnih straneh ponujale brezplačno, čeprav imajo pomembno finančno vrednost, pa je ta prenizka, da bi jo zaračunavali s plačilnimi karticami, po povzetju, naročniškimi sistemi ipd., lahko sedaj tem vsebinam lastniki določijo vrednost, ki jo imajo. Z Moneto je mogoče plačati tudi zneske v višini le nekaj tolarjev.

Sam postopek uporabe Monete je uporabniku prijazen in povsem enostaven. Nakup obsega naslednje korake:

- identifikacija steče v trenutku, ko uporabnik pristopi do vstopnih strani oziroma, ko izrazi zahtevo po plačljivi vsebini. Identifikacijo opravi z vnosom lastne mobilne telefonske številke v predvideno, na novo odprto okence. Kadar uporabnik zahtevo po plačljivi vsebini v eni seji izrazi po že opravljeni identifikaciji, ta ponovno ni potrebna. Identifikacija se namreč opravi le za vsako sejo posebej, tudi če uporabnik med eno sejo obišče spletne strani več ponudnikov vsebin in blaga. Pred identifikacijo uporabnik potrdi tudi strinjanje s Splošnimi pogoji za opravo posla in ceniki;
- na zaslon svojega mobilnega telefona uporabnik v obliki sporočila SMS prejme geslo, ki ga nato vnese v za to predvideno okence. S tem je zagotovljena varnost vsakokratne transakcije, saj uporabnik za vsako sejo prejme novo geslo;
- po potrditvi uporabnik vstopi v sistem plačevanja Moneta ter vstopi na zahtevano plačljivo stran. Ob vstopu lahko opravi tudi nastavitve dolžine seje, maksimalne cene strani ipd;
- strežnik Moneta preveri sejo uporabnika ter posreduje informacijo od ponudnika k uporabniku. Med tem se preveri mesečni limit, stanje na računu, znesek zahtevane informacije ipd;
- če med posredovanjem informacije ne pride do napake, se posredovana informacija zaračuna. Sicer se posredovanje prekine in uporabniku se izpiše obvestilo o napaki.

Nakup s potrditvijo

Tudi nakup s potrditvijo poteka po opisanem postopku. Bistvena razlika je v tem, da se po prenosu plačljive strani kliče ponudnikova potrditvena stran s podpisom, potrditveno kodo in obvestilom o uspešnosti transakcije. Potrditvena stran nato posreduje informacijo o uspešnosti transakcije na strani ponudnika. Tako ponudnik ve, da je uporabnik posredovano stran dobil. Če ponudnikova potrditvena stran napake ne vrne, je celotna transakcija uspela in uporabniku se storitev zaračuna.
Nakup s potrditvijo je primeren v primerih prenosa denarja, vendar je zaradi običajnih visokih zneskov prenosa redkeje uporabljan.

Naročilo

Nakup v obliki naročila se uporablja pri nakupu blaga in je od prejšnjih možnosti nakupa nekoliko drugačen. Namesto direktnega zaračunavanja storitve in izstavitve računa se v tem primeru izdela naročilo, ki ga mora najprej potrditi ponudnik spletne trgovine.

Vendar pa postopek poteka na obstoječi spletni trgovini ne zahteva nobenih tehničnih sprememb. Kupec želene izdelke naloži v nakupovalno košarico, nato pa se odloči za nakup z Moneto. Podatki o košarici se sprejmejo v sistem Moneta, ki kupcu rezervira sredstva, vendar mu vrednosti nakupa še ne zaračuna. Ponudniku je na voljo poseben spletni modul, v katerem lahko pregleduje naročila, ki jih lahko potrdi ali zavrne. V primeru potrditve se kupcu vrednost nakupa zaračuna, ponudnikova obveznost pa je, da potrjeno naročilo dostavi skupaj z računom. Če se nakup zavrne, pa je ponudnikova obveznost, da kupca obvesti o razlogih za zavrnitev.

6.2.2. VARNOST

Ker je Moneta namenjena najširši množici uporabnikov ter ponudnikov storitev in vsebin, zahteva visoke varnostne mehanizme. Zato je varnost sistema zagotovljena tako na psihološki ravni kot tudi na dejanski ravni mehanizmov prenosa podatkov oziroma transakcij.

Prva je dosežena z različnimi mehanizmi, ki uporabnike prepričujejo v varnost sistema. Uporabnik tako lahko sam določi dolžino posamezne seje uporabe (veljavnost "cookija"), ki se nato ob vsakem zaprtju brskalnika prekine, s čimer se "cookie" nikoli ne izpisuje na disk računalnika. Poleg tega prejme obvestilo o tem, kdaj je zahtevana stran dražja od nastavljene vrednosti, lahko si nastavi dnevne in mesečne limite, zahteva stalen izpis informacij, spreminja svoje osebne informacije, poskrbljeno pa je tudi za diskretnost vsakega nakupa.

Varnost sistema je dosežena na različnih ravneh ter na več načinov. Tu gre predvsem za omejevanje dostopa do posameznih nivojev, plačljivih strani in baze podatkov (dostop do tarifikacijskega nivoja na primer poteka preko požarnega zidu, uporabnik plačljive strani na to stran nikoli ni preusmerjen, pač pa jo dobi preko Monete ipd.), enkriptiranje uporabniških imen in gesel, preverjanje avtentičnosti "cookija", zanesljivo strojno opremo in zadostno propustnost povezav na vseh nivojih ipd.

6.2.3. KAKO POSTATI PONUDNIK MONETE

Moneto lahko na svojih spletnih straneh ponudijo vsi ponudniki vsebin in blaga, ki ponujajo storitve in izdelke nižje cenovne vrednosti. Sistem Moneta od ponudnika vsebin ne zahteva finančnih investicij v novo

programsko opremo. Nujen je le prenos spletnih strani na mesto, do katerega ima dostop le Monetin strežnik v Mobitelovem omrežju, ter registracija nove plačljive strani v Monetinem strežniku. Uporabniki do tega novega mesta nimajo dostopa. Poleg tega je potrebno na sosednjih spletnih straneh ponudnika prilagoditi pot do plačniške strani, ki jo po registraciji določi Mobitel.

Pri nakupu s potrditvijo Moneta zaradi prenosa večjih zneskov omogoča tudi potrditev in podpis transakcije. Postopek določitve plačljivega spletnega naslova ostane nespremenjen, nastavitve, ki se nanašajo na potrdilo, pa je treba dodati. Praktično to pomeni, da je treba določiti potrditveni URL, plačljivo stran pa nato poklicati z dodatnim parametrom ConfirmationId="nek_enoličen_id". Ob tem je potrebno poudariti, da uporabnik potrditvenega naslova nikoli ne vidi, prav tako pa klic poteka izključno od Monetinega strežnika do potrditvenega naslova. ConfirmationId mora biti vedno enoličen in se ne sme ponoviti. Če je isti, ga Moneta prepozna in transakcije ne potrdi. Z digitalnim podpisom je onemogočeno zanikanje transakcij s strani Mobitela, z digitalnim podpisom in unikatnostjo ConfirmationId pa podtikanje nikoli izvedenih transakcij s strani ponudnikov ali kupcev.

6.2.4. TEHNIČNE ZAHTEVE MONETE

Kljub nepotrebnosti dodatne tehnične ali programske opreme pa Moneta vendarle zahteva nekaj osnovnih karakteristik strojne in sistemske opreme, ki z zadostno zmogljivostjo omogoča njeno delovanje.

Minimalna konfiguracija podatkovnega strežnika mora biti tako:

- Pentium III 600,
- 256 Mb RAM,
- 20 Gb Disk Raid 5,
- Windows 2000 Server,
- MS SQL 7.0,
- 100 Mbit ethernet.

Minimalna konfiguracija poslovnega in podatkovnega strežnika mora biti:

- Pentium III 600,
- 128 Mb RAM,
- 10 Gb Disk,
- Windows 2000 Server,

- 100 Mbit ethernet.

Na področju komunikacije in varnosti pa so zahteve naslednje:
- vsaj 512 Mbit povezava v internet,
- požarni zid,
- postavitev poslovnega strežnika v varno cono požarnega zida - podatkovni strežnik je v privatnem omrežju,
- povezave z ostalimi sistemi.

6.2.5. POTEK PLAČILA STROŠKOV

Uporabnik po vsakem nakupu v elektronski obliki preko sistema prejme račun nakupa, ki ga izstavi ponudnik, vendar pa uporabnik ni obvezan, da ga pregleda. Uporabnik namreč stroške dejansko poravnava mesečno, in sicer na skupnem zbirnem računu s specifikacijo vseh nakupov pri vseh ponudnikih. Račun uporabniku izda Mobitel.
Vsebina zbirnega računa elektronskih plačil vsebuje zbirni znesek vseh plačil, ki jih izda posamezni ponudnik blaga ali storitev. Uporabnik lahko elektronske račune, ki jih izdajajo ponudniki blaga in storitev, najmanj tri mesece po izdaji računa pregleda tudi na Mobitelovi spletni strani (www.mobitel.si). Ponudnik mora vse račune hraniti v skladu z veljavnimi davčnimi predpisi, tako kot to velja za druge račune, in na način, ki omogoča varno shranjevanje in pregled takih računov. Poleg tega račune določen čas hrani tudi sistem Moneta, vse račune, ki jih po posameznem nakupu prejme preko elektronske pošte, pa je dolžan hraniti tudi uporabnik.

Dnevni in mesečni limit
Vsak uporabnik lahko preko sistema Moneta kupuje v višini določenega dnevnega in mesečnega limita. Če poraba doseže znesek dnevno ali mesečno določenega limita, naročnik sistema GSM v tistem dnevu ali mesecu oziroma do poplačila nastalih obveznosti sistema elektronskih plačil ne bo več mogel. Vse informacije v zvezi z višino dovoljenega dnevnega oziroma mesečnega limita posameznega naročnika družba Mobitel d.d. nudi preko službe za boniteto in izterjavo naročnikov. Naročnik sistema Moneta lahko zahteva povečanje limita za uporabo sistema elektronskih plačil, če ustrezno zavaruje poravnavo zbirnih računov elektronskih plačil.

6.2.6. RAZMERJE MED DRUŽBO MOBITEL D.D. IN PONUDNIKI BLAGA IN STORITEV

Ponudnik z Mobitelom sklene pogodbo za nedoločen čas, na podlagi katere steče tudi priključitev sistemu Monete. Reklamacije, ki zadevajo kvaliteto in količino dobavljenih storitev ali blaga, se naslavljajo direktno na ponudnika storitev ali blaga. Če pa reklamacije prihajajo na Mobitel, jih ta v skladu s Splošnimi pravili napoti na ponudnika. V primeru reklamacij bo preveč plačane zneske uporabniku povrnil ponudnik storitve ali blaga, razen če je družba Mobitel d.d. obremenila uporabnika, ne da bi bil zato izstavljen ustrezen račun ponudnika storitve ali blaga, ki se izda na podlagi vsakokratnega naročila uporabnika.

6.2.7. NEKAJ PRIMEROV UPORABE SISTEMA MONETA

Sistem Moneta je primeren za elektronsko poslovanje podjetij in organizacij najrazličnejših panog. Pazljivost je potrebna le pri izbiri vsebin in izdelkov. Moneta je namreč namenjena izključno plačevanju majhnih zneskov. Temu primerno so določeni tudi limiti nakupov. Naj naštejemo le nekaj primerov internetne ponudbe, plačljive preko Monete. Na področju informacij so možnosti neomejene: preko Monete lahko na primer plačujemo dostop do oglasnih vsebin, poslovnih informacij (npr. poslovnih imenikov, podatkov borznih analitikov ipd.), on-line časopisov in revij, različne spletne storitve (npr. web hosting, dodeljevanje domen, povečanega prostora poštnih predalov itd.), lahko sodelujemo v on-line dražbah ipd. Moneta pa je nenadomestljiva tudi, kadar govorimo o zabavi: pri igrah na srečo, nakupu glasbenih zgoščenk, kaset in drugih glasbenih artiklov, nagradnih igrah, nakupu vstopnic za kino predstave ter druge dogodke ipd.

SKLEP

Večina predstavljenih elektronskih plačilnih sistemov ni nikoli doživela množične, globalne uporabe. Predvsem gre razloge za to iskati v prezapletenosti sistemov, nekompatibilnosti strojne in programske opreme, stroških njihove uporabe in še vedno prisotnem nezaupanju ljudi, da bi kupovali preko svetovnega spleta. Uspešni so bili le tisti sistemi, ki so našli dovolj dober kompromis med varnostjo in prijaznostjo do uporabnika.

Razvoj komunikacij ter združevanje interneta ter mobilnega omrežja prinaša nove možnosti in razsežnosti elektronskega plačevanja. Tehnološki napredek sili ljudi, da se odrekajo starim zakoreninjenim navadam in sprejemajo nove. Internet omogoča podjetjem vstop na svetovni trg, zato se ponudba iz dneva v dan povečuje. Zaradi tega bo iz dneva v dan več kupcev, ki bodo kupovali blago preko interneta, plačevali s plačilnimi karticami, preko mobilnih telefonov in z elektronskim denarjem.

V Sloveniji je uporaba elektronskih plačilnih sredstev še vedno daleč za razvitim svetom. Kljub temu da imamo veliko najrazličnejših plačilnih kartic, jih večina imetnikov uporablja za dvigovanje gotovine na bankomatih. Vendar pa se stanje popravlja in vedno več, predvsem predstavnikov srednje in mlajše generacije, uporablja kreditne kartice. Internetni nakupi pa kljub relativno široki ponudbi ne predstavljajo omembe vrednega deleža med nakupi. Razlogi za to so lahko v ceni blaga, poštnini, carinah ter še vedno nedostopnosti interneta. Kupec se raje odpelje v nakupovalni center, kjer blago lahko vidi in ga preizkusi, kot da bi naročil po internetu.

Rast števila uporabnikov mobilne telefonije močno presega rast števila uporabnikov interneta, zato je nujen razvoj storitev plačevanja blaga in storitev z mobilnim telefonom. V Sloveniji naj bi bilo v tem trenutku že okoli milijon in pol uporabnikov mobilnih telefonov. S sistemi, kot je Moneta, se bo plačevanje blaga in storitev korenito spremenilo in v povezavi s tako imenovanim plastičnim denarjem bo morda nekoč celo ogrozilo obstoj papirnega denarja.

LITERATURA

1. Anghern Albert: The Strategic Implications of the Internet, 1997. [URL:http://www.insead.fr/CALT/Publication/ICDT/strategicImplication.htm], 28. 7. 2002.

2. eCash.com. [URL:http://www.ecash.com/online/], 27. 8. 2002.

3. E-Commerce Security. [URL:http://www.securitytechnet.com/security/ecommerce.html], 20. 9. 2002.

4. Global trust online. Identrus. [URL: http://www.identrus.com/knowledge/pubs/Overview_Brochure.pdf], 4. 9. 2002.

5. Hančič Jan: Kako na Internet. Revija Klik, Ljubljana, junij 2002, 41, 18. str.

6. History of GSM. GSM World. [URL: http://www.gsmworld.com/about/history/index.shtml], 23. 11. 2002.

7. Internet v Sloveniji. RIS. [URL:http://www.ris.org/], 16. 9. 2002.

8. Jerman-Blažič Borka, et al.: Elektronsko poslovanje na internetu. Ljubljana: GV založba, 2001. 206 str.

9. Jerman-Blažič Borka, Klobučar Tomaž, Schneider S. Wolfgang: Advanced security technologies in networking. Amsterdam: IOS Press, 2001a. 257 str.

10. Mihelič Andrej: Dolga pot do brezžičnega. 2002. [URL:http://www.mobimanija.com/claNKI/default.asp?method=page&id=8], 12. 11. 2002.

11. Mobitel UMTS. Mobitel. 2002. [URL:http://www.mobitel.si/umts/index.html], 14. 12. 2002.

12. M-Pay. [URL:http://www.m-pay.com/si/index.php], 4. 10. 2002.

13. Priročnik za uporabo mobilne banke Moba NLB. Nova Ljubljanska banka. [URL:http://www.nlb.si/images/content/_doc/moba-navodila.pdf], 22. 10. 2002.

14. Protocols for secure electronic commerce. Science applicational international corpration. 1997. 73 str.

15. Saje Iztok: Uvod v uvod v mobilno telefonijo NMT-GSM-UMTS. Nova Gorica: Mobilatorij. 2002.
[URL:http://www.mobilatorij.org/mobilatorij/vsebine/a-z/telekomunikacije/mlab3pp.pdf], 3. 12. 2002.

16. SET Secure Electronic Transaction LCC. [URL:http://www.setco.org/], 10.9.2002.

17. Stolpmann Markus: Elektronisches Geld im Internet. Köln: O'Reilly verlag, 1997. 167 str.

18. Survey of electronic money development. Basel: Bank for international settlements, 2000. 111 str.
[URL:http://www.bis.org/publ/cpss38.pdf], 23. 8. 2002.

19. Varno nakupovanje na internetu. SiOL.
[URL:http://nakupi.siol.net/PravneInformacije.asp#kupec], 15. 8. 2002.

20. Zakaj je nakupovanje prek interneta varno?. Eon.
[URL:http://www.eon.si/trgovine/index.jsp], 23. 9. 2002.

21. Zgodovina interneta s Sloveniji. Matkurja.
[http://www.matkurja.com/slo/about/history/], 10. 9. 2002.

22. Welcome to Mondex. Mondex.
[http://www.mondex.com/], 15. 9. 2002.

VIRI

1. Global internet statistic.
[URL: http://www.glreach.com/globstats/], 20.8.2002.

2. How many Online. Nua Internet.
[URL: http://www.nua.ie/surveys/how_many_online/], 16. 9. 2002.

3. Interna gradiva podjetja Mobitel. Moneta.

4. Jelič Borja: Kaj so WAP, GPRS, HSCSD, BlueTooth, MMS, EMS, JAVA… Ljubljana: Mobitel/Mobilatorij 2002. 16 str.

5. Memorandum of understanding : Open Access to Electronic Commerce for European SME's. [URL:http://europa.eu.int/ISPO/ecommerce/MoU/], 17. 8. 2002.

6. Podlipnik Robert, Veber Rok: GSM plačilo. Mobitel. 2001. [URL:http://www.mobitel.si/slo/Press/Predstavitve/2001/Predstavitev13.asp], 30. 11. 2002.

7. Rakovec Domen: Mobilno plačevanje. Mobitel, 2001. [URL:http://www.mobitel.si/slo/Press/Predstavitve/2001/Predstavitev2.asp], 30. 11. 2002

8. Statistični letopis Republike Slovenije 2002. Ljubljana: Statistični urad Republike Slovenije, 2003. 659 str.

9. Šimenc Grega: UMTS-Tretja generacija mobilne telefonije. Ljubljana: Mobitel/Mobilatorij 2002. 21 str.

10. Tasty Bits from the Technology Front: TBTF for 1999-12-16. [URL: http://www.tbtf.com/archive/1999-12-16.html], 27. 8. 2002.

11. Verisign Inc. . [URL:http://www.verisign.com/], 10. 9. 2002.

PRILOGA

SLOVAR IN RAZLAGA POJMOV

Commerce Service Provider (Ponudnik poslovnih internetnih storitev)
CSP pomeni zagotavljati infrastrukturo za spletno poslovanje. Infrastruktura je v tem primeru predvsem varna povezava med trgovcem, kupcem in finančnimi institucijami.

Cookie (piškot)
Majhna datoteka, ki jo spletni strežnik zapiše na odjemalčev računalnik, da bi zbiral informacije, spremljal uporabnikov način uporabe pripadajoče spletne predstavitve ali obiskovalcu prikazoval tiste vsebine, ki si jih je le-ta izbral (personalizacija). Piškoti hkrati omogočajo, da si spletne strani zapomnijo obiskovalce in jih ob naslednjem obisku prepoznajo.

HS/CSD high speed/circuit switched data (hitri/vodovno komutirani podatki)
Sistem za prenos podatkov s pomočjo mobilnih telefonov.

ECC - Elliptic Curve Cryptography
kriptografija javnih ključev z uporabo eliptičnih krivulj.

FTP (File Transfer Protocol)
Standardni protokol, ki nam dovoljuje, da se prijavimo na oddaljeni računalnik, z namenom, da na strežnik ali s strežnika posnamemo določene datoteke.

GPRS - General packet radio service (splošna paketna radijska storitev)
Sistem za prenos podatkov s pomočjo mobilnih telefonov. Nastal je zaradi želje po povezavi interneta z obstoječim mobilnim omrežjem in omogoča višje hitrosti kot prejšnji sistemi.

GPS - Global Positioning System (Sistem za določanje položaja)
Sistem, ki nam s pomočjo oddajnika in satelitov omogoča, da lahko v vsakem trenutku, na katerem koli koncu Zemlje in v vsakem vremenu določiš svoj položaj

HTML (HyperText Markup Language)
Spletni jezik, ki je osnova za gradnjo spletnih strani v Internetu.

HTTP (Hyper Text Transfer Protocol)
Standardni protokol za prenos podatkov med spletnim strežnikom in odjemalcem.

IRC – Internet Relay Chat (Internetna klepetalnica)
Protokol IRC je namenjen znakovnim konferenčnim pogovorom.

Multimedia (Večpredstavnost, multimedija)
Večpredstavnost ali multimedija je kombinacija različnih medijev, kot so zvok in slika ter video.

NMT - Nordic Mobile Telephony
Prva generacija mobilne telefonije.

On-line plačila
Neposredni dostop do plačilnega sistema.

PIN - Personal Identification Number (osebna identifikacijska številka)

POS terminal
POS (Point of Sale) terminal je posebne vrste blagajna, namenjena elektronskemu prenosu podatkov med prodajnim mestom in banko pri plačevanju s plačilnimi karticami.

PGP - Pretty Good Privacy (protokol precejšnje zasebnosti)
Precejšnje zasebnosti. Program za varno elektronsko pošto.

SET - Secure Electronic Transaction (varna elektronska transakcija)

SMS – Short Message System (Sistem kratkih sporočil)

SSL – Secure Socket Layer (sloj varnih vtičnic)
Protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem.

Protokol
Skupek pravil ali dogovorov o načinu komuniciranja.

TCP/IP -transmission control protocol/internet protocol (protokol za krmiljenje prenosa/protokol internet)

URL - uniform resource locator (Naslov vira v enotni obliki)
Naslov dokumenta na internetu.

WAP - wireless application protocol (protokol brezžičnih aplikacij)

WWW – World Wide Web (svetovni splet)