UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

D I P L O M S K O D E L O

ELEKTRONSKI PLAČILNI SISTEMI NA INTERNETU

Ljubljana, junij 2002 **MATIJA PIPAN**

I Z J A V A

Študent _____ izjavljam, da sem avtor tega

diplomskega dela, ki sem ga napisal pod mentorstvom

_____ in dovolim objavo diplomskega dela

na fakultetnih spletnih straneh.

V Ljubljani, dne _____. Podpis:

_____

Kazalo

1. UVOD 2

2. OPREDELITEV ELEKTRONSKIH PLAČILNIH SISTEMOV NA INTERNETU 4

2.1. Zgodovina razvoja elektronskega plačevanja 4

2.2. Ovire v internetnem nakupovanju in plačevanju 7

3. ZAŠČITA IN VARNOST V PODATKOVNIH KOMUNIKACIJAH 19

3.1. Gesla 19

3.2. Kriptografija 20

3.2.1. Simetrična kriptografija 20

3.2.2. Asimetrična kriptografija 21

3.3. Elektronski podpis 22

3.4. Digitalni certifikati 24

3.5. Infrastruktura javnih ključev 25

3.5.1. Struktura PKI 26

3.6. Varni protokoli in sistemi na internetu 27

3.6.1. IPSec – internetni protokol za varen prenos podatkov 27

3.6.2. Protokoli za zaščito transakcij na internetu 28

3.6.3. Varnost na omrežju: Požarni zid 29

3.7. Pametne kartice 30

3.7.1. Zgodovinski razvoj 30

3.7.2. Tehnični podatki 30

3.7.3. Prednosti pametnih kartic 31

3.7.4. Varnost 32

3.8. Fizično varovanje 32

4. VARNI ELEKTRONSKI PLAČILNI SISTEMI 33

4.1. Kreditne in plačilne kartice 33

4.1.1. Varni plačilni sistem SET 34

4.1.2. 3D-SET (Three Domain Model) 37

4.2. Elektronski denar 38
4.2.1. Ecash 39
4.3. Sistem aktivnih plačilnih kartic 41
4.3.1. Mondex 41
4.4. Elektronski ček 42
4.4.1. Elektronski ček podjetja FSTC 43
4.5. Sistem mikroplačil 44
4.5.1. Paynet 44
4.6. Mobilno plačevanje 45

5. ELEKTRONSKO BANČNIŠTVO 46

5.1.1. Klik in ProKlik^{+} – e-bančništvo Nove Ljubljanske banke 48
5.1.2. WAP bančništvo 48
5.1.3. Plačevanje v spletnih trgovinah s Klikom NLB 49

6. ELEKTRONSKI PLAČILNI SISTEMI V SLOVENIJI 50

7. SKLEP 51

8. LITERATURA 52

9. VIRI 53

Kazalo slik in tabel

Slika 1: Simetrična kriptografija uporablja isti ključ za šifriranje in dešifriranje sporočila 20
Slika 2: Asimetrična kriptografija uporablja različna ključa za šifriranje in dešifriranje sporočila.. 21
Slika 3: Primer varnega pošiljanja sporočila z digitalnim podpisom 23
Slika 4: Vsebina digitalnega certifikata..... 24
Slika 5: Struktura EuroPKI 26
Slika 6: Tok podatkov v varnem kanalu SSL 28
Slika 7: Primeri uporabe pametnih kartic..... 30
Slika 8: Čitalnik pametnih kartic..... 31
Slika 9: Raznovrstnost aplikacij, ki jih omogoča pametna kartica SIM v mobilnem telefonu 31
Slika 10: Hierarhija digitalnih certifikatov v sistemu SET 35
Slika 11: Grafični prikaz plačevanja s kreditno kartico preko sistema SET..... 36
Slika 12: Grafični prikaz 3D-SET modela 38
Slika 13: Potek generiranja e-kovancev z uporabo tehnike slepega podpisa 39
Slika 14: Poslovanje z elektronskim denarjem Ecash na internetu..... 40
Slika 15: Potek nakupa z Mondexovo kartico na internetu..... 42
Slika 16: Potek plačila z elektronskim čekom..... 43
Slika 17: Potek plačila z mikroplačilnim sistemom Paynet 45
Slika 18: Potek plačila z mobilnim telefonom in elektronsko denarnico..... 46
Slika 19: Mobilna povezava z banko..... 49

Tabela 1: Pregled dogodkov v obdobju prazgodovine..... 5
Tabela 2: Pregled dogodkov v obdobju pionirstva..... 5
Tabela 3; Pregled dogodkov v obdobju iniciative bančnega sektorja..... 6
Tabela 4: Pregled dogodkov v obdobju internetnih plačilnih sistemov druge generacije 6
Tabela 5: Varnostne zahteve e-kupcev in e-trgovcev pri elektronskem plačevanju..... 8
Tabela 6: Primerjava dolžine ključev ob enaki varnosti..... 22
Tabela 7: Pregled večjih slovenskih bank, ki ponujajo elektronsko bančništvo..... 47
Tabela 8: Večji slovenski spletni trgovci in možni načini plačila e-nakupa..... 50

Pojmovnik

AES	Advanced Encryption Standard	Standard za simetrično šifriranje, ki bo nadomestil DES
B2B	Business to Business	Podjetje – podjetje
B2C	Business to Customer	Podjetje – potrošnik
CA	Certificate Authority	Agencija za certificiranje javnih ključev
CPS	Certification Practise Statement	Izjava o postopkih, ki jih CA uporablja pri izdajanju certifikatov
DES	Data Encryption Standard	Simetrični algoritem za šifriranje
FSTC	Financial Services Technology Corporation	Konzorcij bank in klirinških hiš
GSM	Global System for Mobile Communication	Globalni sistem mobilne telefonije
HTTP	Hyper Text Transport Protocol	Protokol za prenos hiperteksta
HTTPS	Secure http	Varni http
IDEA	International Data Encryption Algorithem	Simetrični algoritem za šifriranje
IP	Internet protocol	Internetni protokol
ISO	International Standard Organisation	Mednarodna organizacija za standardizacijo
MD5		Enosmerna zgoščevalna funkcija
MS	Microsoft	Korporacija Microsoft
P2P	Person to Person	Oseba – oseba
PGP	Pretty Good Privacy	Program za zaščito podatkov
PIN	Personal Identification Number	Zaporedje znakov, ki ga kot geslo uporabimo za dostop do sistema
RA	Registration Authority	Agencija za registracijo
RC4		Simetrični algoritem za šifriranje
RSA		Asimetrični algoritem za šifriranje
SET	Secure Electronic Transaction	Protokol za varne elektronske transakcije
SHA-1	Secure hash Standard	Enosmerna zgoščevalna funkcija
SI-CA		Slovenska agencija za certificiranje javnih ključev
SSL	Secure Socket Layer	Protoko za zaščito podatkov pri prenosu v svetovni splet
SWIFT	Society for Worldwide Interbank Financial Telecommunication	Sistem elektronskega prenosa denarja
TLS	Transport Layer Security	Protokol za zaščito podatkov pri prenosu v svetovni splet
URL	Universal Resource Locator	Naslov vira v enotni obliki
W3C	World Wide Web Consortium	Konzorcij za razvoj in standardizacijo svetovnega spleta
WWW	World Wide Web	Spletne strani
WAP	Wireless Access Protocol	Protokol za brezžični dostop
WTLS	Wireless Transport Layer Security	Protokol za zaščito podatkov pri prenosu v brezžičnem okolju

1. UVOD

Globalizacija, liberizacija ter informatizacija so povzročile premik od nekdaj tradicionalne industrijske družbe v novo informacijsko družbo, kar se kaže v zelo hitrem in intenzivnem razvoju informacijske tehnologije. Če je bil internet v začetku svojega razvoja dostopen le majhnemu krogu ljudi in so ga uporabljali predvsem računalniški zanesenjaki, je v zadnjih nekaj letih doživel velik razmah, predvsem na komercialnem področju. Skoraj že vsak računalnik ima možnost povezave na svetovni splet in tako sedaj ne mine prav veliko časa od prvega zadržanega vstopa v svet medmrežja do prvega opravljenega nakupa v eni izmed e-trgovin na spletu. E-trgovina se od klasične trgovine razlikuje v tem, da stranka s pomočjo spletnega brskalnika na trgovčevem strežniku opravi naročilo ter ga plača. Trgovec nato v najkrajšem možnem času s pomočjo različnih dostavnih služb blago kupcu dostavi. Nakupovanje v e-trgovinah je za kupca udobnejše, saj lahko nakup opravi iz domačega naslonjača, deležen je številčnejših informacij o izdelkih in cenah, sama pestrost ponudbe pa je skoraj neomejena, saj zajema praktično celoten svet. Nakupovanje v e-trgovinah je zelo primerno in dobrodošlo tudi za invalide in starejše ljudi.

Razširjenost uporabe interneta in pogostost nakupovanja v e-trgovinah se po posameznih državah in področjih sveta razlikuje. Po podatkih raziskave podjetja TNS[1] (Taylor Nelson Sofres, četrto največje podjetje za tržne raziskave na svetu) so v letu 2001 skandinavske države prevzele vodilno mesto v številu aktivnih[2] uporabnikov interneta. Na Norveškem je aktivnih uporabnikov interneta kar 63 % celotne populacije, medtem ko znaša svetovno povprečje 31 %. Če pa primerjamo število uporabnikov interneta, ki kupujejo v e-trgovinah, so ZDA krepko v vodstvu, saj kar 33 % njenih uporabnikov redno nakupuje v teh trgovinah. Svetovno povprečje se je v zadnjem letu povečalo za polovico in sedaj znaša okrog 15 % (Global eCommerce Report 2001, 2002).

Razmere v Sloveniji se gibljejo blizu svetovnega povprečja. Po podatkih projekta RIS[3] (Raba interneta v Sloveniji) je v letu 2001 internet uporabljalo približno 25 % celotnega prebivalstva. V spletnih trgovinah pa je nakup opravilo 12 % aktivnih uporabnikov interneta. Leto 2001 predstavlja pomemben mejnik, saj je več kot polovica e-nakupovalcev poleg e-nakupov v tujini opravila nakup tudi v Sloveniji (Nakupovanje, 2001).

Uporabniki interneta radi beremo in poslušamo glasbo. Vsaj tako bi lahko trdili glede na opravljene nakupe v e-trgovinah. Knjige in glasbene zgoščenke so še vedno najbolj priljubljeni artikli e-nakupovalcev. V zadnjem času pa vse bolj pogosto kupujemo tudi oblačila, programsko in strojno računalniško opremo, letalske vozovnice itd.

[1] http://www.tnsofres.com/interactive
[2] oseba, ki je v zadnjem mesecu uporabljala internet
[3] http://www.ris.org

Po tržnih raziskavah podjetja Aqute Research[4] je bilo leta 2001 opravljenih za okrog 48 milijard $ e-nakupov. Ocene za prihodnja leta pa kažejo njihovo strmo naraščanje, saj naj bi v letu 2002 vrednost e-nakupov znašala okrog 70 milijard $, leta 2005 pa že 170 milijard $. Sorazmerno z vrednostjo nakupov pa ne narašča število e-nakupovalcev, saj se le manjšina (15 %) vseh uporabnikov interneta odloča za e-nakupe. Na podlagi raziskave podjetja TNS večjo množičnost e-nakupovanja ovirajo predvsem nezaupanje v varnost tako pri plačevanju kot varovanju podatkov, ki se pošiljajo ob opravljanju nakupa. Ali je ta strah upravičen ali pa gre zgolj za splošno prepričanje in nepoznavanje tehnologij? (Online Purchases Revenues 2000 – 2005, 2002).

Namen diplomskega dela je predstavitev najbolj znanih elektronskih plačilnih sistemov, ki jih e-nakupovalci uporabljajo pri svojih nakupih ter z njimi povezano varnost. Ob tem želim preveriti tudi dogajanje na tem področju v Sloveniji.

Pri izdelavi diplomskega dela sta bili uporabljeni sledeči raziskovalni metodi:

- *teoretična metoda* – študij razpoložljive literature in internetnih virov,
- *empirična metoda* – raziskava in pregled obstoječih varnih elektronskih plačilnih sistemov v Sloveniji.

Na podlagi študija razpoložljive literature in internetnih virov so v poglavjih 2 – 4 predstavljeni najpomembnejši varni elektronski plačilni sistemi, njihova zgodovina ter prikaz varnostnih sistemov v podatkovnih komunikacijah.

Rezultati empiričnih raziskav pa so zajeti v poglavjih 5 in 6, v katerih so predstavljeni elektronsko bančništvo v Sloveniji ter možni načini plačevanja e-nakupov pri slovenskih spletnih trgovcih.

[4] http://www.aqute.com

2. OPREDELITEV ELEKTRONSKIH PLAČILNIH SISTEMOV NA INTERNETU

Dandanes blago in storitve lahko plačujemo na različne načine: z gotovino, čeki, vrednostnimi boni, kreditnimi in bančnimi karticami. To so tako imenovani klasični načini plačevanja. Pri poslovanju in plačevanju na internetu pa uporabljamo elektronske plačilne sisteme. Elektronski plačilni sistemi so pravzaprav klasični načini plačevanja, prilagojeni za uporabo na internetu. Možne oblike so: elektronski denar, elektronski ček, kreditna kartica, elektronski prenos nakazil. Bistvena razlika med obema načinoma plačevanja je v tem, da je v elektronski različici vse digitalno in ni fizičnega kontakta med plačnikom in prejemnikom. V nobeni fazi ni vidna fizična prisotnost plačilnih sredstev. Denarna transakcija se s pomočjo posebnih naprav za povezavo med trgovcem in banko opravi prek interneta ali zasebnega bančnega omrežja.

2.1. Zgodovina razvoja elektronskega plačevanja

(Bohle, 2001, str. 7-18).
Za boljše razumevanje sedanjih trendov na področju elektronskega plačevanja preko svetovnega spleta se je potrebno ozreti v preteklost. Zgodovinski razvoj internetnih plačilnih sistemov lahko razdelimo na štiri temeljna obdobja:

- *obdobje prazgodovine,*
- *obdobje pionirstva,*
- *iniciativa bančnega sektorja,*
- *internetni plačilni sistemi druge generacij.*

Obdobje prazgodovine (1976 – 1992)
Še predno se je internet dodobra uveljavil in postal nepogrešljiv pri elektronskem poslovanju, je bilo kar nekaj poskusov razvoja različnih sistemov elektronskega plačevanja. Mednje lahko štejemo POS terminale[5], e-denar (programsko in strojno podprt), e-denarnice, predplačilne eno-namenske kartice[6] in mikroplačila. Za to obdobje je bil značilen predvsem razvoj predplačilnih eno-namenskih pametnih kartic, ki so nasledile magnetne kartice iz 70-tih let. S posplošitvijo te eno-namenskosti je prišlo leta 1992 do uvedbe prve e-denarnice, Danmønt. To obdobje traja vse do konca leta 1992, ko število uporabnikov interneta naraste na milijon.

[5] POS (Point of sale) – omogoča avtorizacijo kartice ter transakcijo elektronskega plačila
[6] primer je telefonska kartica, na kateri so shranjeni telefonski impulzi

Tabela 1: Pregled dogodkov v obdobju prazgodovine

Leto	Dogodek
1976	Diffie in Hellmann: začetek kriptografije javnega ključa
1978	Prva predplačilna magnetna telefonska kartica v Belgiji
1982	D. Chaum : objava študije o *'slepem podpisu'*, ki je pomembna za anonimnost plačil
1983	Prva predplačilna telefonska pametna kartica v Franciji (Telecarte)
1984	Minitel – uvedba mikroplačil
1989	Ustanovitev podjetja DigiCash na Nizozemskem
1991	Začetek razvoja Mondex-a v Veliki Britaniji
1992	Uvedba e-denarnice Danmønt na Danskem

Vir: Bohle, 2001, str. 9.

Obdobje pionirstva (1993 – 1995)

Druga faza je s stališča varnosti zelo vplivala na nadaljnji razvoj internetnega plačevanja. Podjetje Netscape[7] je leta 1994 predstavil protokol SSL[8], ki omogoča varen prenos podatkov med kupčevim brskalnikom in trgovčevim strežnikom. Vse do tega trenutka so se informacije o kreditnih karticah in bančnih računih pošiljale preko interneta popolnoma brez zaščite in so bile lahka tarča nepridipravov. V tem obdobju je podjetje DigiCash[9] preizkusil prvo varno metodo plačevanja, imenovano Cyberbucks. Cyberbucks je bil prvi poizkus tako imenovanega 'internetnega denarja', katerega izdajatelj ni banka, temveč podjetje samo. Na trgu se pojavita še podjetji First Virtual Holding in Cyber Cash[10] Inc., ki opravljata vlogo posrednika med kupci, trgovci in izdajatelji kreditnih kartic. Zanimanje za elektronsko plačevanje začne kazati tudi bančni sektor.

Tabela 2: Pregled dogodkov v obdobju pionirstva

Leto	Dogodek
1994	Razvoj SSL s strani podjetja Netscape
1994	Prihod podjetij First Virtual in Cyber Cash
1994	Uvedba elektronskih kovancev Cyberbucks podjetja DigiCash

Vir: Bohle, 2001, str. 10.

Iniciativa bančnega sektorja (1995 – 1998)

V obdobju pionirstva je bančni sektor izgubil nadzor nad internetnimi plačilnimi sistemi, zato si je prizadeval z novimi iniciativami ponovno prevzeti vodilno vlogo na tem področju. Pomemben korak k temu je bil razvoj protokola za varno transakcijo SET (Secure Electronic Transaction), ki se uporablja za elektronsko plačevanje s kreditnimi karticami. Bančni sektor je v tem času tudi prilagodil tradicionalne plačilne instrumente za uporabo na internetu. V letu 1998 nekatera 'pionirska' podjetja na področju internetnega plačevanja zaidejo v finančne težave.

[7] http://www.netscape.com
[8] SSL (Secure Sockets Layer)
[9] http://www.digicash.com
[10] http://www.cybercash.com

Tabela 3; Pregled dogodkov v obdobju iniciative bančnega sektorja

Leto	Dogodek
1995	Banka Mark Twain ponudi plačilni sistem Ecash podjetja DigiCash
1996	Prva transakcija preko protokola SET (Secure Electronic Transaction)
1997	Uvedba e-denarnice v Belgiji
1998	Izdaja e-denarja pod vplivom regulacije bančnega sistema v Nemčiji
1998	Prenehanje delovanja podjetja First Virtual
1998	Bankrot podjetja DigiCash

Vir: Bohle, 2001, str. 11.

Internetni plačilni sistemi druge generacije (1999 →)

Dandanes plačevanje s kreditnimi karticami, odvisno od države do države, zavzema med 70 in 93 % vseh internetnih plačil. V prihodnje naj bi se ta trend nekoliko obrnil v drugo smer, na pomembnosti naj bi pridobili internetni plačilni sistemi, kot so elektronske denarnice, e-denar, P2P[11]. Ti plačilni sistemi vidijo svojo priložnost predvsem v skupinah ljudi, ki nimajo svojega bančnega računa ali kreditnih kartic, ter med tistimi, ki želijo popolno anonimnost plačevanja. Pomembno vlogo v internetnem plačevanju v zadnjem času pridobivajo mobilni telefoni in z njimi povezani plačilni sistemi.

Tabela 4: Pregled dogodkov v obdobju internetnih plačilnih sistemov druge generacije

Leto	Dogodek
1999	Razvoj plačilnih sistemov P2P (npr. PayPal)
1999	Pojav virtualnih denarnih računov (npr. Cash+)
2000	Prenehanje plačilnega sistema CyberCash v Nemčiji
2000	Predstavitev plačilnega modela 3D-SET
2001	Bankrot podjetja CyberCash

Vir: Bohle, 2001, str. 12.

[11] P2P (Person to Person) - transakcije med fizičnimi osebami

2.2. Ovire v internetnem nakupovanju in plačevanju

Trije najpogostejši razlogi, ki odvračajo ljudi od e-nakupovanja in hkrati uporabe elektronskih plačilnih sistemov, so: *nevarnost zlorabe kreditne kartice, zloraba osebnih podatkov* in *nezaupljivost do e-trgovcev*. Skupni imenovalec vseh treh razlogov je *vprašljiva varnost*.

Pomanjkanje zaupanja in varnosti predstavlja tako največjo oviro za še hitrejši razvoj elektronskega poslovanja. V klasični trgovini med kupcem in trgovcem obstaja vrsta varnostnih mehanizmov, ki zagotavljajo zaupanje in občutek varnosti. Kupec lahko izdelke vidi, jih prime, preizkusi, je v neposrednem stiku s trgovcem. Znesek lahko plača z gotovino, čekom ali kreditno / bančno kartico. Pri plačilu s kreditno / bančno kartico račun potrdi z lastnoročnim podpisom ali pa v posebno napravo vnese PIN[12] kodo. Kupec ima tako ves čas celoten pregled nad nakupom in plačilom, kar za e-nakupovanje in e-plačevanje, kjer je vse virtualnega[13] značaja, ne moremo trditi.

Zadovoljivo varnost in zaupanje pri internetnem trgovanju lahko dosežemo ne le z zamenjavo klasičnih varnostnih mehanizmov z novimi digitalnimi, temveč tudi z razvijanjem novih orodij (digitalnih, pravnih in proceduralnih). S tem zmanjšamo tveganje, ki je prisotno pri elektronskem poslovanju na internetu.

Zahteve e-kupcev in e-trgovcev pri elektronskem plačevanju

Elektronski plačilni sistemi morajo tako kot klasični načini izpolnjevati določene varnostne zahteve, ki so bistvenega pomena za uspešno e-poslovanje. Varnostne zahteve e-trgovcev in e-kupcev pri elektronskem plačevanju na internetu se nanašajo na *zaupanje med strankama, neokrnjenost podatkov, verodostojnost, odgovornost* in *preprečitev tajenja komunikacij*[14] (glej tabelo 5, na str. 7).

[12] PIN (Personal Identification Number) – identifikacijska številka uporabnika, dolžine 4-12 številk
[13] navidezno, nevidno
[14] non - repudiation

Tabela 5: Varnostne zahteve e-kupcev in e-trgovcev pri elektronskem plačevanju

	E-kupec	**E-trgovec**
Zaupanje	Moji osebni podatki in podatki o plačilu morajo biti zaščiteni pred zlorabo (med samo transakcijo in tudi po njej v trgovčevi bazi podatkov).	Moji poslovni podatki morajo biti zaščiteni pred zlorabo.
Neokrnjenost	Podatki o plačilu se med samo transakcijo ne smejo spreminjati brez moje vednosti.	Podatki o plačilu se med samo transakcijo ne smejo spreminjati brez moje vednosti.
Verodostojnost	Želim preveriti, ali je e-trgovec res tisti, za katerega se izdaja, je vreden zaupanja?	Želim preveriti ali je e-kupec res tista oseba za katero se izdaja, je upravičen do uporabe plačilnega instrumenta (npr.: je kreditna kartica res njegova), je plačilno sposoben?
Odgovornost	V primeru kraje denarja zaradi tuje krivde ne želim nikakršne odgovornosti in le omejeno, če je krivda moja.	V primeru kraje denarja ne želim nikakršne odgovornosti.
Preprečitev tajenja Komunikacije	Imam možnost odstopa od plačila v primeru, da: ☞ trgovec ni opravil dogovorjenega, ☞ izdelek/storitev ni enaka opisu, ☞ se premislim.	Imam zagotovilo, da kupec ne bo prekinil plačila po prejetju izdelka ali storitve.

Vir: Centeno, 2001.

Med zahtevami e-kupcev in e-trgovcev je opaziti določeno simetrijo, vendar pa prihaja tudi do razlik predvsem v povezavi z verodostojnostjo in preprečitvijo tajenja komunikacije.

Poleg že naštetih zahtev e-kupec pogosto izrazi željo po tajnosti posla. Anonimnost je potrebna predvsem pri medorganizacijskih nakupih, kjer ne želimo, da za nakup izve konkurenca, nakupih na internetnih straneh namenjenih samo za odrasle, itd. Plačilo z gotovino zagotovi potrebno anonimnost. Za plačnikom se izgubi sled. Račun, ki ga prejmemo ob plačilu, je le potrdilo, da je bila neka stvar kupljena, ne vemo pa, kdo je kupec (Centeno, 2001).

Vse te osnovne zahteve, ki zagotavljajo varno elektronsko plačevanje podobno klasičnemu, so z današnjo tehnologijo in obstoječo infrastrukturo tehnično izvedljive.

3. ZAŠČITA IN VARNOST V PODATKOVNIH KOMUNIKACIJAH

Za sodobno informacijsko okolje je značilna porazdeljena arhitektura, v kateri nimamo enega ali več osrednjih računalnikov, ampak množico osebnih računalnikov in strežnikov povezanih v globalno omrežje – internet, pri katerem pa se vse bolj izpostavlja problem varnosti. V svetu elektronskega poslovanja prežijo na uporabnike in ponudnike storitev drugačne nevarnosti kot v klasičnem poslovanju, zato so potrebni tudi drugačni varnostni ukrepi in orodja. Za zagotovitev varnosti imamo na voljo različne kombinacije programske in strojne opreme ter fizično varovanje. Njihova izbira je določena z varnostno politiko in je odvisna od stopnje zahtevane zaščite in oblike sistema. E-trgovina in z njo povezano elektronsko plačevanje poteka preko interneta, zato je varnost temeljni predpogoj za uspešno poslovanje.

3.1. Gesla

V elektronskem poslovanju se z gesli srečujemo praktično na vsakem koraku. Predstavljajo najenostavnejši način identifikacije uporabnika in so ključ dostopa do varovanih podatkov. Iz sledečih razlogov varovanje z gesli uvrščamo med šibko zaščito:

- Uporabniki si večinoma izbirajo gesla, ki si jih je lažje zapomniti. Takšna gesla pa je žal tudi lažje razkriti. Uganjevanje tujih gesel poteka s pomočjo elektronskih slovarjev, s poznavanjem uporabnikovih podatkov in s preizkušanjem že uporabljenih gesel,
- Pri identifikaciji razkrijemo svoje geslo in tako omogočimo naslovniku, da se izdaja pod našim imenom,
- Gesla se ponavadi prenašajo v nešifrirani obliki in so tako lahka tarča napadalcev. Tudi če so gesla predhodno šifrirana, jih napadalec lahko prestreže in uporablja v takšni obliki za kasnejše predstavljanje.

Zaradi navedenih razlogov šibko overjanje s pomočjo gesel ni primerno za preverjanje identitete v elektronskem poslovanju, razen za dostop do lokalnega sistema ali aktiviranje določenih naprav (pametne kartice, internetnega brskalnika …).

Uporabnost gesel v javnih omrežjih lahko povečamo z enkratnimi gesli. Posamezno geslo se uporabi le enkrat, zato prestrezanje gesel tu nima pravega pomena. Pri tem načinu je zelo pomembno, da se iz preteklih gesel ne da izračunati prihodnjih gesel. Najbolj znan način za identifikacijo s pomočjo enkratnih gesel je uporaba kartice, ki vsebuje mikroprocesor in ekran ter je sinhronizirana z uro na strežniku. Lastnik kartice, ki želi izkazati svojo identiteto, vtipka na kartici geslo za njeno uporabo, algoritem pa nato na podlagi trenutnega časa generira geslo, katerega uporabnik pošlje na strežnik. Takšen način identifikacije svojih komitentov pri elektronskem bančništvu sta pred časom uporabljali Dolenjska banka in SKB banka (Jerman Blažič, 2001, str. 115).

3.2. Kriptografija

Kriptografija se že stoletja uporablja za zaščito zaupnih podatkov, ki jih je potrebno poslati iz ene lokacije na drugo. Kadar govorimo o kriptografiji, mislimo na šifriranje podatkov v takšno obliko, da nepooblaščeni uporabniki ne morejo razbrati njihove vsebine. V preteklosti je bila kriptografija v domeni vojske, z razvojem javnih računalniških omrežij in vse večjega števila uporabnikov pa je postala nepogrešljiva tudi na tem področju. S pomočjo kriptografskih sistemov lahko dosežemo verodostojnost, tajnost in nezmožnost tajenja sporočila.

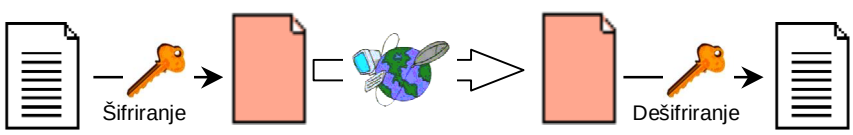
Kriptografski sistem sestavljata dva dela: *kriptografski algoritem* in *šifrirni ključ*. Kriptografski algoritem je matematična funkcija, ki podatke s pomočjo šifrirnega ključa spremeni v nepooblaščenim osebam neberljivo obliko. V preteklosti so bili algoritmi tajni, saj je že njihovo poznavanje zadostovalo za dešifriranje sporočila, dandanes pa so kriptografski algoritmi večinoma poznani in dostopni vsakomur, skriti morajo ostati le šifrirni ključi. Število možnih ključev pri algoritmu je odvisno od dolžine ključa (8-bitni ključ omogoča 2^8=256 možnih numeričnih kombinacij, kar je tudi število različnih ključev). Stopnja varnosti algoritmov za šifriranje je odvisna od dolžine ključa. Ključa dolžine 128 bitov s pomočjo metode preizkusa vseh možnih kombinacij (brute-force) z našim osebnim računalnikom ne najdemo v nekaj milijonih letih (Jerman Blažič, 2001, str. 102).

V grobem ločimo dve vrsti kriptografskih sistemov: ***simetrične*** in ***asimetrične***

3.2.1. Simetrična kriptografija

Simetrična kriptografija uporablja en sam skrivni ključ za šifriranje in dešifriranje. Problem pri simetričnem šifriranju je, kako varno razdeliti šifrirne ključe pooblaščenim osebam. Pošiljatelj sporočila se mora z vsakim prejemnikom posebej dogovoriti, kje je skrivni ključ, kar pa povečuje možnost, da kdo ta skrivni ključ prestreže in dešifrira sporočilo. Prednost simetričnega šifriranja je v njegovi hitrosti. V današnjem času se uporablja predvsem v kombinaciji z drugimi algoritmi, ki omogočajo varno izmenjavo ključev. Najbolj znan standard za simetrično šifriranje je DES (Data Encryption Standard), ki pa ga zaradi prekratkih ključev danes ni več tako zelo varno uporabljati. Pomembnejši algoritmi so še IDEA, 3DES, RC2, RC4 in v zadnjem času AES (256 bitni ključ) (SET Secure Electronic Transaction Specification – Bussines Description, 1997).

Slika 1: Simetrična kriptografija uporablja isti ključ za šifriranje in dešifriranje sporočila



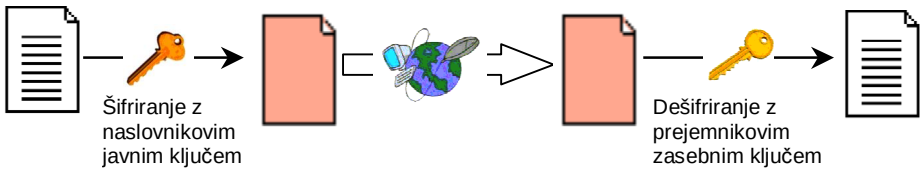
Vir: SET Secure Electronic Transaction Specification. Book 1: Business Description, 1997.

3.2.2. Asimetrična kriptografija

Asimetrična kriptografija je znana tudi kot kriptografija javnih ključev (PKC)[15]. Začetnika v asimetrični kriptografiji sta bila W. Diffie in M. Hellman, ki sta leta 1976 prvič predstavila koncept javne kriptografije. Koncept kriptografije javnega ključa temelji na paru ključev: en ključ je namenjen šifriranju, drugi pa dešifriranju sporočila. Vsak uporabnik ima tako dva ključa: *zasebni ključ* in *javni ključ*. Javni ključ se ponavadi nahaja na strežniku in je dostopen vsakomu, zasebni ključ pa je varno shranjen pri njegovem lastniku. Ključa sta matematično sorodna, a se med seboj toliko razlikujeta, da je na podlagi enega ključa nemogoče odkriti drugega. Najpogosteje uporabljen asimetrični kriptografski algoritem je RSA[16], ki temelji na zelo velikih praštevilih. V zadnjem času na pomembnosti pridobivajo asimetrični algoritmi na podlagi eliptičnih krivulj. Njihova prednost pred RSA je predvsem večja hitrost ob enaki stopnji varnosti.

Pri asimetrični kriptografiji pošiljatelj zaupno sporočilo šifrira z naslovnikovim javnim ključem. Naslovnik, ki ima edini ustrezen zasebni ključ, lahko dešifrira sporočilo. Če želimo zagotoviti še neokrnjenost sporočila in verodostojnost pošiljatelja, uporabimo postopek digitalnega podpisovanja, ki ga omogoča kriptografija javnih ključev.

Slika 2: Asimetrična kriptografija uporablja različna ključa za šifriranje in dešifriranje sporočila



Vir: SET Secure Electronic Transaction Specification. Book 1: Business Description, 1997.

Prednost kriptosistemov javnih ključev pred simetrično kriptografijo je v enostavnem razpošiljanju ključev. Javni ključ lahko brez kakršnegakoli strahu, da bo ta prestrežen, pošljemo osebam, s katerimi želimo varno komunicirati, ali pa ga le-te preprosto snamejo s posebej za ta namen prirejenih strežnikov. Slabost asimetričnih kriptosistemov v primerjavi s simetričnimi je predvsem v hitrosti šifriranja in overjanja javnih ključev. Hitrost šifriranja je odvisna od dolžine ključa. Šifriranje in dešifriranje z 1028 bitnim ključem pri RSA, ki zagotavlja podobno stopnjo varnosti kot 72 bitov dolg ključ pri simetričnih algoritmih, je nekajkrat počasnejše. Zaradi te pomanjkljivosti daljša sporočila običajno šifriramo s simetričnimi kriptoalgoritmi, ključe za te algoritme pa zaščitimo z asimetričnimi. Kriptosisteme, sloneče na javnih ključih, tako uporabljamo pri šifriranju večinoma le za razdeljevanje ključev (SET Secure Electronic Transaction Specification – Bussines Description, 1997).

[15] PKC (Public Key Cryptography)
[16] RSA – asimetrični kriptografski algoritem, ki je dobil ime po začetnicah avtorjev: Ron Rivest, Adi Shamir in Leonard Adleman

Tabela 6: Primerjava dolžine ključev ob enaki varnosti

Dolžina ključa v simetričnem šifriranju	Dolžina javnega ključa v asimetričnem šifriranju
56 bitov	384 bitov
64 bitov	512 bitov
80 bitov	768 bitov
112 bitov	1792 bitov
128 bitov	2304 bite

Vir: Centeno, 2001.

3.3. Elektronski podpis

Elektronski podpis je posebej za elektronsko poslovanje izdelan sistem, ki nadomesti lastnoročni podpis in je namenjen predvsem za preverjanje neokrnjenosti podatkov, verodostojnosti pošiljatelja ter preprečevanje tajenja. Za elektronsko podpisovanje obstaja več različnih metod:

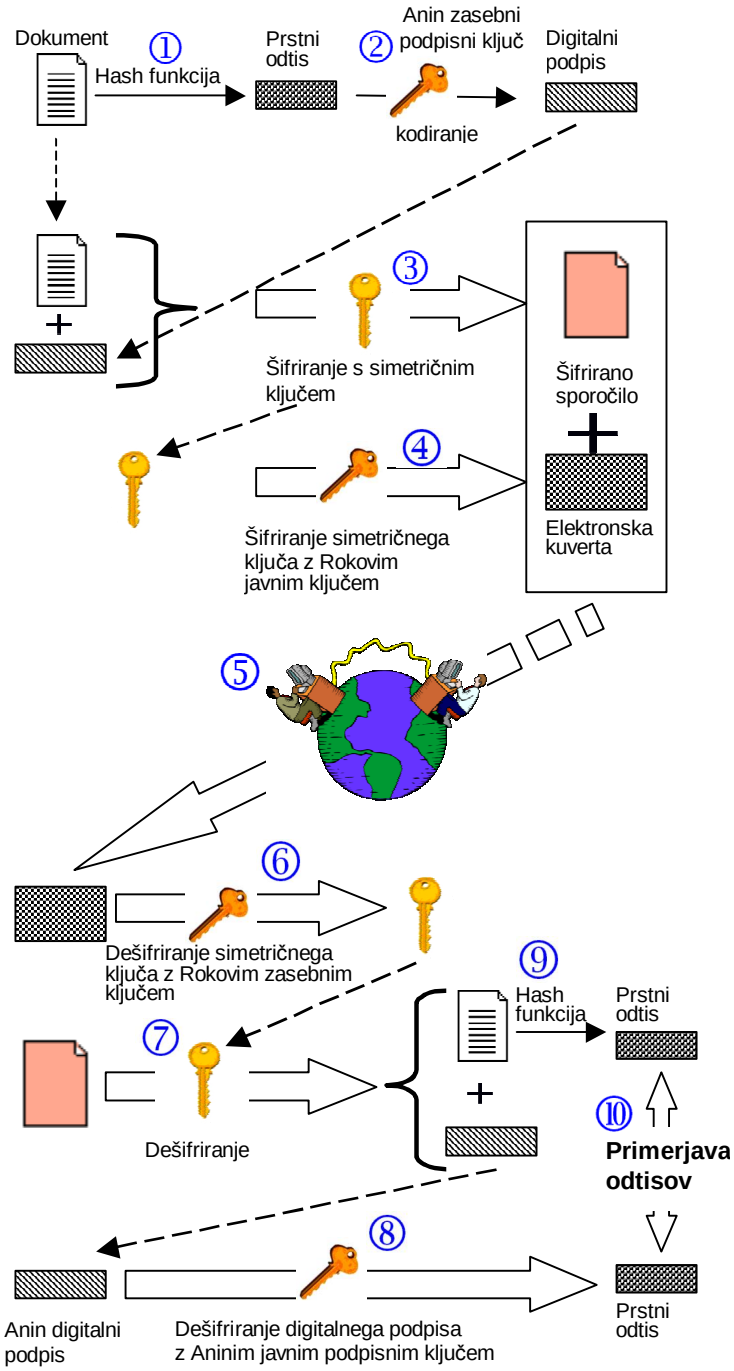
- *vključevanje slike lastnoročnega podpisa v dokument,*
- *podpisovanje z elektronskim peresom,*
- *metode na podlagi simetričnih kriptografskih algoritmov (MAC [17]),*
- *digitalno podpisovanje s pomočjo metod javne kriptografije.*

Vse metode v primerjavi z lastnoročnim podpisom zagotavljajo neokrnjenost podpisanega dokumenta. Najvišjo stopnje varnosti pa zagotavlja ***digitalni podpis***, ki temelji na asimetrični kriptografiji. Enako kot pri kriptografiji javnih ključev ima uporabnik dva ključa: *javni ključ* in *zasebni ključ*. Uporabimo lahko isti par ključev kot pri asimetričnem šifriranju, vendar to ni priporočljivo, saj so varnostne zahteve v obeh primerih precej različne. Ponavadi ima uporabnik še en par ključev, ki je namenjen le za digitalno podpisovanje.

Postopek digitalnega podpisovanja poteka v dveh korakih. Sporočilo najprej skrčimo z eno izmed enosmernih zgoščevalnih funkcij[18] v bloke enakih dolžin. Z zgostitvijo sporočila v konstantno velike bloke namreč uničimo pomen sporočila in ga je nemogoče rekonstruirati v prvotno obliko. Vsaka najmanjša sprememba v izvornem sporočilu povzroči spremembo vsebine bloka. Posamezni blok[19] predstavlja *'prstni odtis'* sporočila, ki ga šifriramo še z zasebnim podpisnim ključem, in tako dobimo digitalni podpis. Za preverjanje digitalnega podpisa prejemnik uporabi javni podpisni ključ podpisnika, s katerim dešifrira blok. Prejemnik nato še sam izračuna vrednost enosmerne zgoščevalne funkcije podpisanega sporočila in primerja bloka. Če sta bloka popolnoma enaka, je pošiljatelj res oseba, za katero se izdaja in poslano sporočilo med prenosom ni bilo spremenjeno (Centeno, 2001).

[17] MAC (Message Authentication Code)
[18] one-way-hash functions – enosmerna zgostitvena funkcija
[19] message digest – povzetek sporočila 160 ali 128 bitni numerični prikaz sporočila

Slika 3: Primer varnega pošiljanja sporočila z digitalnim podpisom



1. Ana z enosmerno zgoščevalno funkcijo preslika dokument v blok konstantne dolžine – prstni odtis.
2. Povzetek dokumenta šifrira s svojim zasebnim podpisnim ključem.
3. Ana naredi simetrični ključ, s katerim nato šifrira celoten dokument in digitalni podpis. Ta ključ bo Rok potreboval za dešifriranje dokumenta in digitalnega podpisa. Uporaba simetričnega ključa je smiselna zaradi bistveno večje hitrosti šifriranja.
4. Za zagotovitev varnega prenosa simetričnega ključa ga Ana šifrira z Rokovim javnim ključem, ki ga je dobila na strežniku ali pa ga ji je poslal Rok. Šifriran simetrični ključ spravi v elektronsko kuverto.
5. Ana pošlje Roku sporočilo, ki vsebuje simetrično šifriran dokument ter digitalni podpis in asimetrično šifriran simetrični ključ.
6. Rok dešifrira elektronsko kuverto s svojim zasebnim ključem. S tem postopkom pridobi simetrični ključ, ki ga potrebuje za dešifriranje dokumenta in digitalnega podpisa.
7. Rok s simetričnim ključem dešifrira dokument in digitalni podpis.
8. Dešifriranje digitalnega podpisa z Aninim javnim podpisnim ključem, ki ga je dobil na strežniku ali pa ga mu je poslala Ana.
9. Rok z enosmerno zgoščevalno funkcijo preslika enak dokument v blok konstantne dolžine – prstni odtis.
10. Na koncu primerja prstna odtisa. Če sta odtisa enaka ima zagotovilo, da je dokument res poslala Ana. Enakost odtisov potrjuje tudi neokrnjenost dokumenta.

Vir: SET Secure Electronic Transaction Specification. Book 1: Business Description, 1997.

Diagram prikazuje celoten pregled nad procesom varnega pošiljanja dokumenta preko javnega omrežja (internet). Na prvi pogled se proces varnega pošiljanja zdi zelo zapleten, vendar v praksi to poteka avtomatizirano in je zanj potreben le pritisk na gumb.

Programi za šifriranje običajno uporabljajo več kriptografskih algoritmov. PGP[20] (Pretty Good Privacy) uporablja algoritme RSA, IDEA in MD5, odvisno od tega, ali šifriramo dokument, se digitalno podpisujemo ali kaj tretjega (Jerman Blažič, 2001, str. 106).

3.4. Digitalni certifikati

(Ward, 1999, str. 23-32; Digital Certificates, 2002; Jerman Blažič, 2001, str. 109-111).
Kriptografija na osnovi javnega ključa temelji na paru ključev. Par ključev lahko generiramo sami, in sicer s programi kot so internetni brskalnik, programi za elektronsko pošto ter drugi. Ko sta ključa izdelana, lastnik poskrbi za ustrezno zaščito zasebnega ključa, javni ključ pa po elektronski pošti razpošlje osebam, s katerimi želi varno komunicirati. Tak način generiranja ključev ni najboljši, saj se ne zagotavlja verodostojnosti pošiljatelja. Pošiljatelj lahko generira par ključev v imenu neke druge osebe, za katero se izdaja, in naslovnik tako ne more biti povsem prepričan, ali je pošiljatelj res oseba, za katero se izdaja.

Da se tem težavam izognemo, je overjanje javnih ključev temeljni pogoj za zagotavljanje verodostojnosti pri asimetrični kriptografiji. Overjanje javnih ključev opravljajo agencije za certificiranje javnih ključev CA[21]. CA izda lastniku javnega ključa digitalno podpisano potrdilo – *digitalni certifikat*, s katerim zagotavlja drugim uporabnikom verodostojnost ključa. Pri uporabi javnega ključa moramo najprej preveriti veljavnost certifikata ter ostale podatke, zapisane v njem. Če certifikat od časa izdaje ni bil spremenjen ali preklican, ga lahko uporabimo. Zelo pomembno je naše zaupanje v CA, da res izdaja certifikate le pravim lastnikom javnih ključev.

Slika 4: Vsebina digitalnega certifikata

Vir: Jerman Blažič, 2001, str. 110.

[20] http://www.pgp.com - verzija PGP-ja, ki se ne sme izvažati izven ZDA in Kanade
http://www.pgpi.com - mednarodna verzija PGP-ja, ki se lahko izvaža po vsem svetu
[21] CA (Certification Authority) – agencija za certificiranje javnih ključev

Certifikate lahko, glede na preverjanje podatkov lastnika ob izdaji, razvrstimo v štiri razrede, ki so opredeljeni z varnostno politiko CA na njenem strežniku. Za certifikate prvega razreda se preverja le elektronski in klasični naslov lastnika. Pri certifikatih drugega razreda CA preveri osebni dokument, pri certifikatih tretjega razreda se preveri še lastnikova kreditna kartica. Certifikat četrtega razreda vsebuje tudi podatke o položaju znotraj organizacije oziroma premoženjskem stanju lastnika.

Agencijo za certificiranje javnih ključev lahko ustanovijo tako vladne ustanove kot komercialne organizacije. CA poleg izdajanja certifikatov vzdržuje tudi bazo preklicanih in neveljavnih certifikatov, kjer lahko uporabnik preveri veljavnost certifikata. CA mora pri svojem delu izpolnjevati tudi vrsto varnostnih zahtev, kot so:

- delovna postaja CA mora biti dobro fizično varovana,
- povezava z omrežjem je omejena in strogo varovana,
- CA ne sme nuditi drugih storitev,
- upravljanje delovne postaje iz omrežja ne sme biti možno,
- zasebni ključ CA mora biti shranjen na pametni kartici, sicer CA ne sme biti priključena na omrežje,
- CA za podpisovanje uporablja par ključev, narejenih z algoritmom RSA, dolžine vsaj 1024 bitov.

3.5. Infrastruktura javnih ključev

(Public Key Cryptography Infrastructure, 2002).
Infrastruktura javnih ključev (PKI[22]) je kombinacija programske in strojne računalniške opreme ter politike in pravil certificiranja. Osnovna naloga PKI je omogočiti varno elektronsko poslovanje uporabnikom, ki se med seboj ne poznajo in želijo varno komunicirati. PKI temelji na digitalnih certifikatih, s katerimi potrdimo uporabnikov elektronski podpis in njegov javni ključ. PKI kot celoten sistem za uporabo asimetrične kriptografije v elektronskem poslovanju lahko združuje naslednje subjekte in dokumente:

- agencija za certificiranje (CA),
- agencija za registracijo (RA),
- politika certificiranja,
- sistem distribucije certifikatov,
- dokument o ravnanju s certifikati (CPS – Certification Practice Statement).

Agencija za certificiranje (CA)

Osnovna naloga CA je izdajanje, varovanje in vzdrževanje certifikatov. Zaupanje v PKI temelji na CA.

Agencija za registracijo[23] (RA)

Ti uradi predstavljajo posrednika med CA in uporabnikom. RA od naročnika, ki zaprosi za certifikat, pobere podatke in jih preveri. Po končani registraciji naročnika pošlje CA zahtevo za izdajo digitalnega certifikata. Zelo pomembno je zaupanje CA v verodostojnost podatkov, ki jih dobi od RA.

[22] PKI (Public Key Infractuture)
[23] RA (Registration Authority)

Politika certificiranja

V grobem ločimo dve politiki certificiranja: politiko certificiranja v globalnih PKI, ki ureja odnose med CA, RA, lastniki in uporabniki certifikatov, ter politiko certificiranja v posameznih organizacijah z lastno CA. Politika certificiranja v organizaciji določa stopnjo zahtevane varnosti in vključuje dokumente, s katerimi so predpisani postopki ravnanja s ključi in drugimi pomembnimi podatki.

Sistem distribucije certifikatov

Certifikati so lahko distribuirani na več načinov. Izmenjajo si jih lahko uporabniki sami; le-ti se nahajajo na strežniku v organizaciji ali pa na posebnem strežniku v javnem omrežju. Način distribucije je odvisen od strukture PKI.

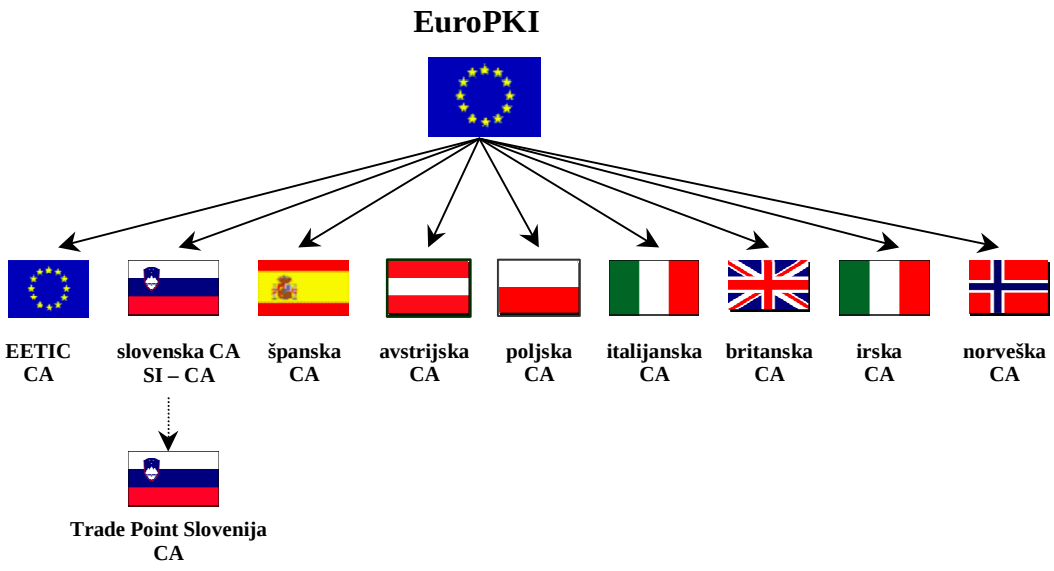
Dokument o ravnanju s certifikati (CPS)

CPS je dokument, ki definira natančne postopke izvajanja politike certificiranja v praksi in vsebuje opis strukture CA ter njenih nalog. V njem so nadrobno opredeljeni postopki izdaje, sprejetja in preklica certifikata ter njegove distribucije. CPS je posebno pomemben pri komercialnih CA (CCA-Commercial Certificate Authority), saj iz njega lahko razberemo, koliko zaupanja je vredna posamezna CA.

3.5.1. Struktura PKI

Ključi se lahko uporabljajo za različne namene in v različnih okoljih (elektronsko bančništvo, državna uprava, medorganizacijsko poslovanje, vojska …). Vsako okolje zahteva različno stopnjo varnosti in specifično strukturo PKI, zato ni pričakovati enotne PKI. Infrastrukture med seboj niso povezane, večina jih vsebuje le eno ali nekaj CA. Ena redkih PKI, katerih namen je združevanje CA iz različnih držav, je EuroPKI.

Slika 5: Struktura EuroPKI



Vir: http://www.europki.org

Vrhovna agencija EuroPKI[24] deluje v Italiji. Del te infrastrukture je tudi slovenska agencija za certificiranje SI-CA[25], katera podpisuje javne ključe drugih slovenskih overiteljev. V Sloveniji ustanavljajo svoje CA še Center vlade RS za informatiko[26] (SIGEN CA – izdaja kvalificirana digitalna potrdila za državljane ter za pravne in fizične osebe; SIGOV CA – izdaja kvalificirana digitalna potrdila za institucije javne uprave), Trade Point Slovenija[27] (ustanovljen s strani Ministrstva za gospodarske dejavnosti, del EuroPKI) in nekatere komercialne organizacije (NLB – izdaja CA svojim klientom za varno poslovanje v elektronskem bančnem sistemu KLIK[28]) (Jerman Blažič, 2001, str. 111).

3.6. Varni protokoli in sistemi na internetu

Varnost elektronskega poslovanja na internetu lahko zagotovimo na različnih ravneh. Najpogosteje to storimo na aplikacijski, transportni in omrežni ravni. V prvem primeru že sama aplikacija vsebuje varnostne mehanizme (program za elektronsko pošto, internetni brskalnik). V drugih dveh primerih pa varujemo podatke tako, da med računalnikoma vzpostavimo varen kanal, ki zagotavlja zaupnost, neokrnjenost podatkov ter možnost preverjanja identitete.

3.6.1. IPSec – internetni protokol za varen prenos podatkov

Najbolj znana metoda za zaščito podatkov na omrežni ravni je standard IPSec[29]. IPSec nam omogoča vzpostavitev navideznega zasebnega omrežja znotraj javnega omrežja, kot je internet. Vzpostavitev navideznega zasebnega omrežja zahteva precej manj stroškov, kot izgradnja zasebnega omrežja. Izmenjava podatkov med dvema ali več oddaljenimi računalniki poteka v šifrirani obliki in je digitalno podpisana. Pri standardu IPSec so vsi podatki varovani na ravni IP, ne glede na to, ali uporabljamo aplikacije z vgrajenimi varnostnimi mehanizmi ali ne. IPSec združuje dva varnostna mehanizma: AH (Authentication Header) in ESP (Encapsulating Security Payload). Prvi zagotavlja neokrnjenost in overjanje podatkov. ESP pa vedno zagotavlja neokrnjenost in zaupnost, po želji pa tudi overjanje podatkov. Oba varnostna mehanizma lahko uporabljamo skupaj ali ločeno.

Izmenjava ključev pri standardu IPSec lahko poteka ročno, ko administrator sistema ročno vstavi potrebne ključe v sistem za komunikacijo, ali pa avtomatično, ko se računalniki sami dogovorijo za skupen ključ. Avtomatično izmenjavo ključev nam omogoča protokol IKE (Internet Key Exchange), ki za identifikacijo predvideva uporabo digitalnih certifikatov (Jerman Blažič, 2001, str. 118).

[24] http://www.europki.org
[25] http://www.si-ca.org
[26] http://www.sigov.si/cvi/
[27] http://ca.tradepoint.si/
[28] https://klik.n-lb.si/
[29] IPSec (IP Security Protocol), http://www.ietf.org/html.charters/ipsec-charter.html

3.6.2. Protokoli za zaščito transakcij na internetu

Za varen prenos transakcij v javnem omrežju, kot je internet, se najpogosteje uporabljajo sledeči protokoli:

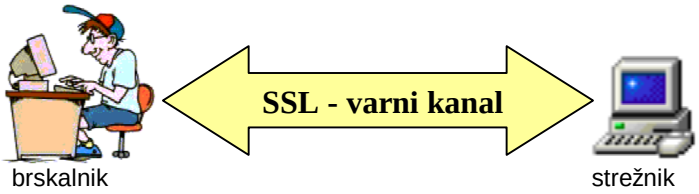
- SSL (Secure Sockets Layer),
- TLS (Transport Layer Security),
- WTLS (Wireless Transport Layer Security) – za transakcije preko brezžičnih povezav.

Skupna značilnost vsem trem protokolom je vzpostavitev varnega kanala med internetnim brskalnikom in strežnikom. Vsem podatkom, ki se izmenjujejo v tem varnem kanalu, je zagotovljena zaupnost, neokrnjenost in verodostojnost. Najbolj znan protokol je SSL, ki ga je leta 1998 razvilo podjetje Netscape in potrdil W3C[30] (World Wide Web Consortium). Širom sveta ga uporabljajo banke pri elektronskem bančništvu, nepogrešljiv pa je tudi pri elektronskih plačilnih sistemih. Protokol SSL je sestavni del aplikacij, kot sta brskalnika MS Internet Explorer in Netscape.

Protokol SSL je sestavljen iz dveh delov:

- *SSL Handshake Protocol* – njegova naloga je preverjanje verodostojnosti strežnika in uporabnika ter prenos digitalnih certifikatov in simetričnih ključev. Omogoča tudi usklajevanje algoritmov
- *SSL Record Protocol* – zagotavlja neokrnjenost podatkov ter šifriranje

Slika 6: Tok podatkov v varnem kanalu SSL



Vir: Young, 1998, str. 14.

Strežnik in brskalnik pri vzpostavitvi povezave najprej preverita verodostojnost drug drugega, nato pa uskladita kriptografske algoritme ter varno izmenjata asimetričen ključ za morebitno kasnejše šifriranje. Dolžino ključev in vrsto kriptografskih algoritmov lahko določimo sami. Izbiramo lahko med *simetričnimi algoritmi* (DES, 3DES, RC4 in AES), *enosmernimi zgoščevalnimi funkcijami* (SHA-1 in MD5) ter *asimetričnim algoritmom* RSA. Po končanem postopku preverjanja identitete, usklajevanja kriptografskih algoritmov ter izmenjave ključev lahko brskalnik in strežnik začneta s pomočjo SSL Record Protokola s pošiljanjem podatkov. Podatkom, ki potujejo znotraj varnega kanala, je vedno zagotovljena njihova neokrnjenost. Če pa želimo zagotoviti še zaupnost, jih še dodatno šifriramo (Young, 1998, str, 12-18).

Uporabo protokolov SSL in TLS na internetu lahko prepoznamo po predponi *https* namesto *http*. Primer uporabe teh protokolov je elektronski bančni sistem Klik Nove ljubljanske banke: https://klik.n-lb.si .

[30] http://www.w3.org/

Z uporabo protokola SSL lahko zagotovimo varen prenos podatkov, ne moremo pa zagotoviti njihove varnosti na strežniku ali brskalniku. Pri nakupovanju v spletni trgovini lahko kupec s pomočjo protokola SSL varno pošlje svojo številko kreditne kartice trgovcu, nima pa nikakršnega zagotovila o kasnejšem varovanju številke s strani trgovca. Kupec mora zaupati trgovcu, da bo številko kasneje varno shranil pred morebitnimi napadalci oziroma je ne bo sam zlorabil. Podobno moramo storiti tudi sami in zaščititi naš računalnik pred nepooblaščenim dostopom (SET Secure Electronic Transaction Specification. Book 1: Bussines Description, 1997).

3.6.3. Varnost na omrežju: Požarni zid

Na internetu, tako kot tudi v drugih okoljih naše družbe, so prisotni ljudje, ki s svojimi dejanji želijo škodovati nam ali organizacijam. Takšni ljudje vdirajo preko javnega omrežja v varovana omrežja, kjer uničujejo, poneverjajo ali kradejo zaupne podatke. S sistemom požarnega zidu (firewall) lahko omejimo dostop do varovanega omrežja. Lastnosti požarnega zidu so odvisne od politike kontrole dostopa, katera je del varnostne politike.

Požarni zidovi nas ščitijo pred nepooblaščenimi uporabniki od 'zunaj' in opravljajo vlogo nekakšnega filtra. Nekateri požarni zidovi dovolijo le promet z elektronsko pošto in tako varujejo naše omrežje pred vsemi napadi, razen tistimi z elektronsko pošto. Ostali požarni zidovi so manj restriktivni in blokirajo le tiste, pri katerih so možni problemi. Bolj kompleksni zidovi preprečujejo dostop od zunaj, omogočajo pa nemoteno komuniciranje od znotraj na ven.

Slabost požarnih zidov je v tem, da ne preverjajo uporabnika, temveč le IP naslov in številko protokola, ter na podlagi teh informacij odločajo, ali bodo dovolili komunikacijo ali ne. Nemočni so tudi pred zlorabami zaposlenih znotraj omrežja, saj lahko ti preko telefonskega omrežja, faksa ali na disketah oziroma CD-jih odnašajo zaupne podatke. Večina požarnih zidov ne preverja prisotnosti virusov v podatkih, ki se pretakajo preko njega, kar pomeni, da ni zagotovila o neokrnjenosti in zaupnosti podatkov.

Ločimo dva tipa požarnih zidov:

- *Požarni zidovi na omrežni ravni* – ugotavljajo IP naslov in številko protokola. Podatki se pretakajo iz interneta direktno skozi njih v varovana omrežja in obratno.
- *Požarni zidovi na aplikacijski ravni* – požarni zidovi se postavljajo v posebej za to načrtovane proxy strežnike[31]. Ta prestreže IP paket in spusti aplikacijo (elektronska pošta) le uporabnikom, ki imajo dovoljenje za njihovo uporabo.

Požarni zidovi sami ne zagotavljajo zadostne varnosti, zato so poleg njih potrebni še nekateri drugi varnostni sistemi za potrebe varovanja omrežja (Curtin, 2000).

[31] proxy strežnik – strežnik, ki se nahaja med zasebnim zaščitenim omrežjem in internetom. Njegova naloga je preprečitev direktnega pretoka podatkov med dvema omrežjema

3.7. Pametne kartice

3.7.1. Zgodovinski razvoj

V prvo generacijo plačilnih kartic sodijo 'papirnate kartice'. Kmalu potem so jih zamenjale plastične kartice z reliefno izpisanimi številkami, kar je pomenilo že prvo stopnjo avtomatizacije. Naslednja generacija plačilnih kartic so bile magnetne kartice, na katere je že možno elektronsko shraniti določene podatke, in so v uporabi še danes. Z razvojem magnetnih kartic se je zvišal nivo avtomatizacije in varnosti. Leta 1974 so v Franciji magnetni kartici dodali še čip in tako je nastala prva pametna kartica[32]. Do prve masovne uporabe pametnih kartic je prišlo leta 1985, ko so francoske banke poslale na trg 16 milijonov teh kartic. Temu trendu je leto dni kasneje sledil francoski telekom z vpeljavo sedmih milijonov pametnih telefonskih kartic. V Evropi je bila ta vrsta kartic zaradi visokih stroškov telekomunikacij pri on-line verifikaciji transakcij hitro vsesplošno sprejeta. Pametne kartice omogočajo verifikacijo tudi off-line, kar močno zniža stroške pri enaki stopnji varnosti. V ZDA, kjer so stroški telekomunikacij majhni, so se pametne kartice uveljavile nekoliko kasneje. Trenutno je po ocenah strokovnjakov v uporabi že 3,6 milijarde pametnih kartic po vsem svetu (Newman, 1999).

3.7.2. Tehnični podatki

Pametna kartica je plastična kartica z vgrajenim mikročipom, kateri lahko sprejema, shranjuje in procesira podatke ter omogoča uporabo različnih aplikacij. Pametne kartice se poleg plačevanja uporabljajo tudi v mobilnih telefonih GSM (SIM kartica[33]), predplačilnem telefoniranju, nadomeščajo zdravstvene izkaznice, osebne izkaznice, na njih shranjujemo digitalne certifikate itd.

Slika 7: Primeri uporabe pametnih kartic

Kreditna kartica MasterCard | Zdravstvena izkaznica ZZZS | Plačilna kartica Mercator Pika | Telefonska kartica Telekoma Slovenije | SIM kartica mobilnega telefona

V primerjavi s karticami z magnetnim zapisom imajo pametne kartice kar nekaj prednosti:

- *nanje je moč shraniti od desetkrat do celo stokrat več informacij,*
- *omogočajo precej večjo varnost pri njihovi uporabi,*
- *omogočajo procesiranje in izvajanje zapletenih algoritmov.*

Za prenos podatkov z ali na kartico potrebujemo čitalnike pametnih kartic. Kartico vstavimo v napravo in že se lahko začne komunikacija med čipom in terminalom. Pred tem je potrebno še predhodno vtipkati identifikacijsko številko PIN (Personal Identification Number), ki je skrita

[32] smart card
[33] SIM (Subscriber Identity Module)

v čipu in preko katere čitalnik prepozna lastnika kartice. Na trgu so tudi že pametne kartice, ki za prenos podatkov ne potrebujejo fizičnega kontakta s čitalnikom. Te kartice se po izgledu ne razlikujejo od drugih pametnih kartic. Razlika je le v notranjosti, kjer imajo vgrajeno anteno, s pomočjo katere se brezžično povežejo s čitalnikom.

Slika 8: Čitalnik pametnih kartic

Vir: http://www.eps.no/offer.htm

Na svetu je veliko proizvajalcev pametnih kartic in čitalnikov, zato je mednarodna organizacija za standardizacijo (ISO[34]) predpisala standarde[35]. Standardi določajo obliko kartice in električne povezave (predpisuje mesta na sprednji strani kartice, kjer morajo biti priključki takšni, da je kartica združljiva z vsakim avtomatom oziroma čitalnikom). Standardi pa ne omejujejo procesorske moči, dokler se čip prilega mestu pod kontaktno ploščico (Newman, 1999).

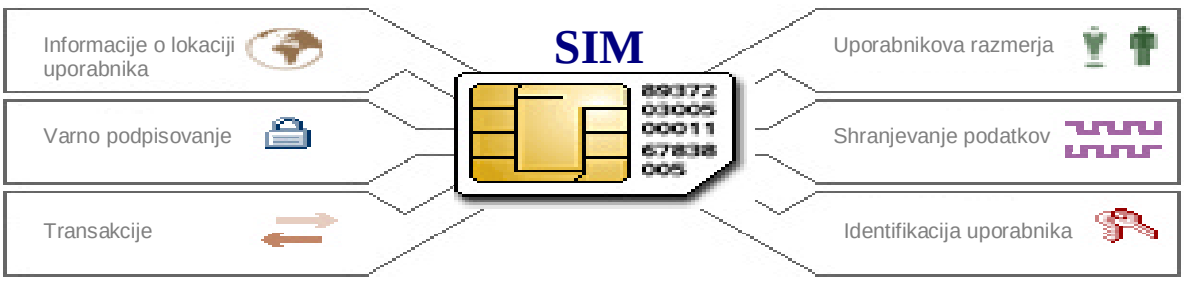
3.7.3. Prednosti pametnih kartic

Pametne kartice imajo pred drugimi karticami vrsto edinstvenih prednosti tako za uporabnika kot za izdajatelja kartic.

Mnogovrstnost aplikacij

Pametna kartica uporabniku omogoča združitev več različnih aplikacij na eni sami kartici. Ta posebnost je za lastnika takšne kartice zelo dobrodošla, saj zmanjšuje število kartic v njegovi denarnici. Tako lahko eno samo pametno kartico uporabljamo kot kombinacijo kreditne kartice in elektronske denarnice. Podobno tudi SIM kartica v mobilnem telefonu lahko združuje vrsto različnih aplikacij (komunikacijo, shranjevanje podatkov, določitev lokacije ...)

Slika 9: Raznovrstnost aplikacij, ki jih omogoča pametna kartica SIM v mobilnem telefonu



Vir: http://www.smarttrust.com/sim/default.asp

[34] http://www.iso.ch - ISO (International Organization for Standardization)
[35] ISO standardi, ki predpisujejo obliko in lastnosti pametnih kartic so: ISO 7810 – 7813 in ISO 7816

3.7.4. Varnost

Na področju varnosti plačevanja s kreditnimi karticami pomeni razvoj pametne kartice velik napredek. Njena visoka stopnja varnosti temelji na:

- *nezmožnosti poneverjanja* – s kartice je nemogoče fizično prekopirati zasebni ključ,
- *omogoča izkazovanje verodostojnosti in procesiranje kriptografskih algoritmov.*

Izkazovanje verodostojnosti uporabnika je ena najpomembnejših komponent zagotavljanja varnosti. Pri pametnih karticah izkazujemo verodostojnost s številko *PIN* ali pa z uporabo *biometričnih metod*. Za uporabo kartice moramo poznati PIN. V primeru kraje kartice ima tat le nekaj poizkusov uganitve pravilnega PIN-a, nato pa se kartica sama trajno zaklene. Prav tako lahko kartico ob prijavi izgube zaklene tudi njen izdajatelj. Še večjo varnost nam omogočajo biometrične metode, ki za izkazovanje verodostojnosti lastnika zahtevajo preverjanje prstnega odtisa ali očesne šarenice, katere podatki so shranjeni v čipu na kartici.

Pametne kartice omogočajo tudi različne kriptografske tehnike, kot so šifriranje, dešifriranje podatkov ter procesiranje kriptografskih algoritmov in šifrirnih ključev.

Vsi ti varnostni ukrepi postavljajo pametne kartice v sam vrh varnega elektronskega poslovanja. Pomembno pa se je tudi zavedati, da napadi na varnostne sisteme niso danes nič novega in nenavadnega, zato nam pametne kartice ob vsej tej varnostni tehnologiji ne morejo zagotavljati 100 % varnosti (The Smart Card, 2002).

3.8. Fizično varovanje

Poleg vseh programskih varnostnih sistemov in tehnologij je za varno elektronsko poslovanje zelo pomembno tudi fizično varovanje. Podjetje lahko v izgradnjo varnostnega sistema investira veliko denarja in kupi najnovejšo tehnologijo, vendar če pri tem zanemari fizično varovanje, naredi podobno delo, kot če bi na slamnato hiško montirali neprebojna metalna vrata.

Pod pojmom fizično varovanje razumemo varovanje fizičnega dostopa do vitalnih delov informacijskega sistema in komunikacijske opreme. Osrednji računalniki, strežniki in druge komunikacijske naprave morajo biti v posebnem prostoru. Vstop v ta prostor mora biti varovan, saj nam lahko nekdo nepooblaščeno odtuji strojno ali programsko opremo in podatki so izgubljeni. Dostop v ta prostor imajo lahko le pooblaščeni delavci. Priporočljivo je tudi, da se zapisujejo vsi vstopi v komunikacijski prostor ter vse dejavnosti, ki so bile izvedene. Fizično varovanje obsega tudi ožičenje internega omrežja, ki mora biti takšno, da onemogoča nepooblaščene priključitve in možnost prisluškovanja.

4. VARNI ELEKTRONSKI PLAČILNI SISTEMI

Plačilna sredstva, ki se uporabljajo na internetu, so zasnovana tako, da opravljajo enake ali podobne naloge kot klasične oblike plačevanja, in so pravzaprav elektronske različice klasičnih plačilnih sredstev. Za plačevanje na spletu poznamo več vrst osnovnih elektronskih plačilnih sistemov:

- ***kreditne in debetne kartice,***
- ***elektronski denar,***
- ***sistem aktivnih plačilnih kartic,***
- ***elektronski ček,***
- ***sistem mikroplačil,***
- ***mobilno plačevanje,***
- ***elektronsko bančništvo.***

4.1. Kreditne in plačilne kartice

Kreditne in debetne kartice so brez dvoma najpomembnejše plačilno sredstvo na internetu, saj njihov delež med vsemi plačilnimi sistemi zavzema okoli 85 % (Gartner 2001[36]). Vodilni podjetji na tem področju sta Visa in MasterCard.

Pri plačevanju s karticami poznamo več vrst izvedbe plačila:

- naročilo po pošti / telefonu (MO / TO)[37],
- nevarovana plačila po omrežju,
- varni plačilni sistemi.

Naročilo po pošti / telefonu

MO / TO način kupovanja in plačevanja s karticami na internetu uvrščamo med začetne oblike trgovanja na spletu. Kupec svoje naročilo, podatke o kartici in naslovu pošlje trgovcu po pošti ali pa jih sporoči po telefonu. Pomanjkljivost te oblike plačevanja je vprašljiva varnost. Kupec nima zagotovila, da je podatke o kartici poslal pravemu trgovcu in ne lažnemu. Na drugi strani pa trgovec nima zagotovila, da bo kupec naročeno blago plačal, saj nima njegovega podpisa. Kljub tem pomanjkljivostim se ta način plačevanja marsikje uporablja še danes.

Nevarovana plačila po omrežju

Nevarovana plačila po omrežju se srečujejo s podobnimi problemi kot MO / TO. Napadalci lahko s posebnimi programi prestrežejo podatke o karticah, jih shranijo na svoj računalnik ter jih nato zlorabijo. Zaradi elektronskega načina potekajo vsi postopki hitreje in predno je kraja ugotovljena, je povzročena škoda lahko že velikanska (O'Mahony, Peirce, Tewari, 2001, str. 63).

Prav zaradi takšnih pomanjkljivosti so različna podjetja razvila varne načine plačevanja s karticami na internetu. Podjetje CayberCash je 1994 med prvimi razvilo in ponudilo varno

[36] http://www3.gartner.com/Init
[37] MOTO (mail order / telephone order)

plačevanje prek interneta. Danes pa sodi med najbolj dovršene varne sisteme plačevanja s karticami SET in njegova novejša različica 3D-SET.

4.1.1. Varni plačilni sistem SET

(Get SET, 2002).
Najbolj znan sistem za elektronsko plačevanje s kreditno kartico na internetu je protokol za varno transakcijo SET (Secure Electronic Transaction). SET sta leta 1997 razvili podjetji MasterCard International[38] in Visa[39] v njunem skupnem podjetju SETco[40]. Pri izgradnji sistema SET je sodelovalo tudi nekaj najbolj znanih podjetij s področja informacijske tehnologije, kot so IBM, Microsoft, Baltimore Technologies, Globeset in Verisign. Osnovni namen SET-a je zagotovitev varnega prenosa informacij o plačilu preko zasebnega in javnega omrežja, kot je internet. SET danes predstavlja pomemben mejnik v varnem internetnem plačevanju s kreditno kartico, saj vzbuja zaupanje in občutek varnosti vseh udeležencev v procesu plačevanja.

Udeleženci in potrebna orodja v sistemu SET

Pri plačevanju s kreditno kartico v sistemu SET so vedno udeležene štiri stranke:

- *kupec – lastnik kreditne kartice,* [41]
- *kupčeva banka, ki je izdala kartico ,*[42]
- *trgovec,*
- *trgovčeva banka .*[43]

Orodja, ki jih potrebuje lastnik kartice

Za uporabo sistema SET mora lastnik kreditne kartice predhodno od svoje banke, katera mu je kartico izdala, pridobiti:

- *digitalno denarnico,*
- *digitalni certifikat, pametno kartico ali kakšno drugo identifikacijsko orodje.*

Digitalna denarnica ali elektronska denarnica opravlja podobne naloge kot običajna denarnica. V njej so shranjeni identifikacijski podatki o lastniku kartice, digitalni certifikat,
številke kreditnih kartic, računi ter druge informacije, ki so dosegljive, kadar lastnik kartice nakupuje v spletnih trgovinah. Digitalna denarnica, ki jo ima lastnik kartice shranjeno na svojem računalniku, imenujemo klientova denarnica 44. Digitalna denarnica pa je lahko shranjena tudi na strežniku banke in jo imenujemo strežniška denarnica 45.

[38] http://www.mastercardintl.com
[39] http://www.visaeu.com
[40] http://www.setco.org
[41] (Cardholder) – lastnik kartice, ki nakupuje v e-trgovinah
[42] (Issuing bank) – kupčeva banka, ki ima licenčno pogodbo z MasterCardom in izdaja kartice svojim komitentom
[43] (Acquiring bank) – trgovčeva banka, ki ima licenčno pogodbo z MasterCardom in opravlja bančne transakcije trgovcev
[44] Client Wallet
[45] Server Wallet

Digitalni certifikat omogoča identifikacijo lastnika kartice. Izda ga kupčeva banka in je shranjen v digitalni denarnici lastnika kartice. **Orodja, ki jih potrebuje trgovec**
Za uporabo sistema SET mora trgovec pridobiti:

- SET-ovo POS programsko opremo,
- digitalni certifikat.

POS (Point – of – sale) programska oprema omogoča trgovcu sprejemanje transakcij s strani kupcev in njihovo kasnejšo izpeljavo preko svoje banke (trgovčeve banke). SET-ova programska oprema podpira vse vrste elektronskega plačevanja: kreditne kartice, debetne kartice, pametne kartice ter mobilno plačevanje.

Trgovčev ***digitalni certifikat*** identificira trgovca in hkrati izkazuje odnos med trgovcem in njegovo banko. Digitalni certifikat pridobi trgovec od svoje banke.

Orodja, ki jih potrebuje trgovčeva banka

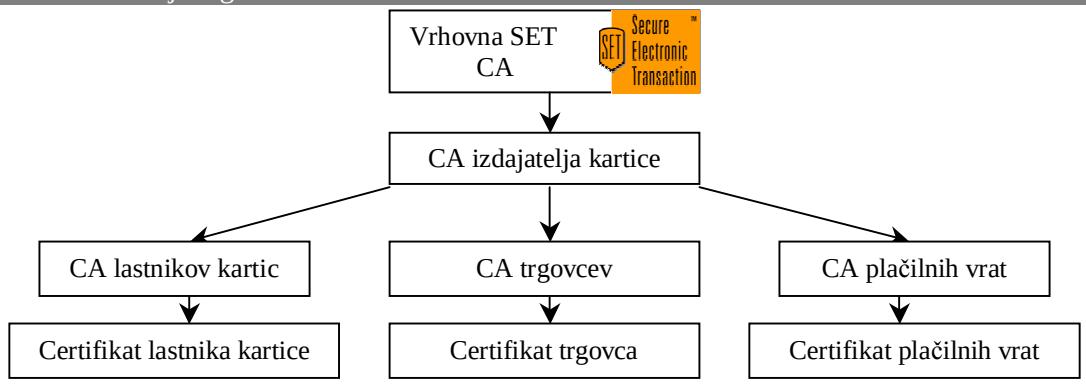
Trgovčeva banka mora imeti ***plačilna vrata*** (payment gateway), skozi katera se prenašajo SET-ova sporočila, kot so podatki o plačilu, identifikacijski podatki udeležencev in informacije o naročilu. Glavna naloga plačilnih vrat je sprejemanje sporočil s strani trgovca in kupčeve banke ter njihovo pravilno razvrščanje in usmerjanje. Vsi podatki so zaradi zagotavljanja maksimalne varnosti šifrirani.

Hierarhija izdajanja digitalnih certifikatov v sistemu SET

Za zagotavljanje varnosti je zelo pomembna premišljena infrastruktura izdajanja digitalnih certifikatov in šifrirnih ključev. SET predvideva tristopenjski model:

- Vrhovna SET CA – *podpisuje certifikate podjetjem, ki izdajajo kartice*,
- CA podjetij, ki izdajajo kartice (MasterCard, Visa, Cyber-COMM, PBS International) – *podpisujejo certifikate CA lastnikov kartic (CCA), CA trgovcev (MCA) in CA plačilnih vrat (PCA)*,
- CCA – *podpisuje certifikate lastnikom kartic*, MCA – *podpisuje certifikate trgovcem* in PCA – *podpisuje certifikate plačilnim vratom (npr. trgovčevi banki).*

Slika 10: Hierarhija digitalnih certifikatov v sistemu SET



Vir: SET Secure Electronic Transaction Specification. Book 1: Business Description, 1997.

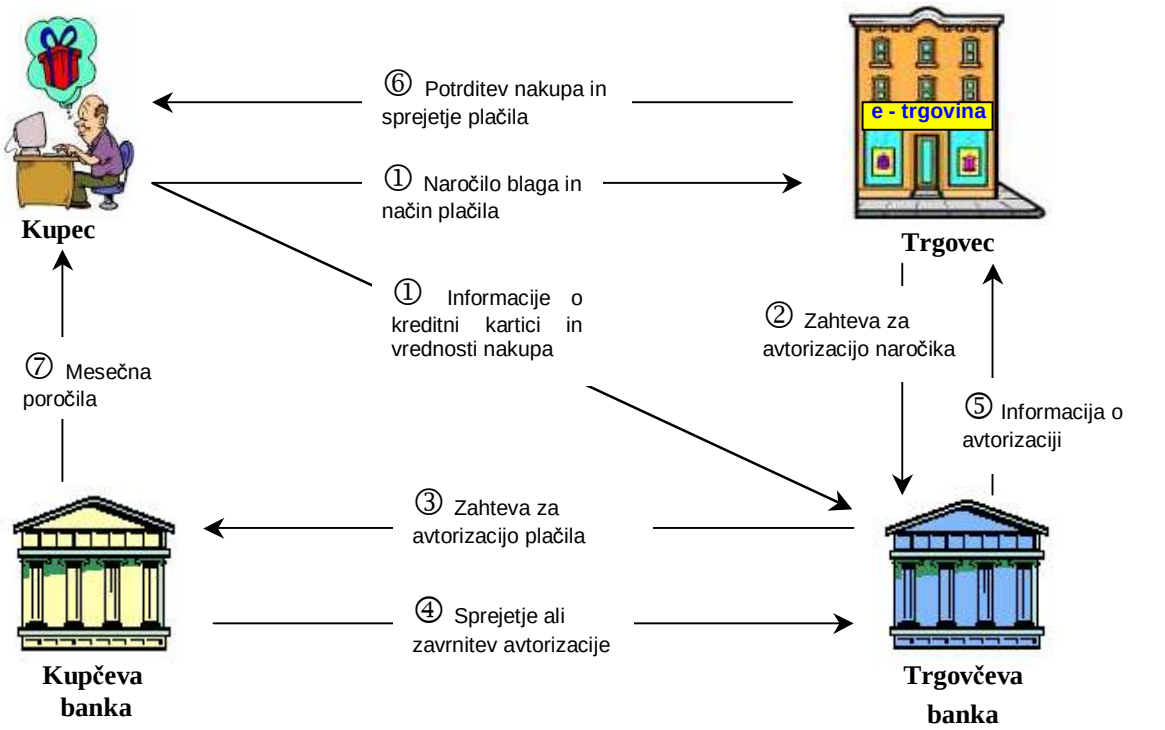
Potek transakcije v sistemu SET

V vsaki transakciji s kartico v sistemu SET sodelujejo štiri stranke: kupec, trgovec, kupčeva banka in trgovčeva banka.

Potek transakcije v sistemu SET:

1. Proces transakcije v SET-u se prične, ko kupec v e-trgovini izbere željene izdelke in jih položi v virtualno košarico[46] ter potrdi svoje naročilo. Digitalna denarnica dokonča naročilo in ga pošlje naprej.
2. SET avtomatsko šifrira vse kupčeve podatke o naročilu ter informacije o kreditni kartici in vrednosti naročila s 1024 bitnim ključem. Tako šifrirani podatki so zaščiteni pred zunanjim prestrezanjem. Kupec ne pošlje trgovcu nobenega podatka, preden se ta pravilno ne identificira.
3. V SET-ovem toku informacij trgovec prejme le kupčevo naročilo in specifikacijo načina plačevanja, vse ostale informacije o plačilu pa so poslane *plačilnim vratom* trgovčeve banke. V trgovčevi banki dešifrirajo kupčeve informacije o plačilu in trgovčevo zahtevo za avtorizacijo naročila.
4. Plačilna vrata v trgovčevi banki preverijo tudi pristnost kupčevega in trgovčevega certifikata. To ne varuje kupca le pred morebitno zlorabo podatkov, kadar ti potujejo po internetu, temveč tudi pred morebitno krajo goljufivega trgovca.
5. Trgovčeva banka pošlje zahtevo za avtorizacijo naročila kupčevi banki.
6. Kupčeva banka preveri veljavnost kartice in kreditno sposobnost kupca ter pošlje odgovor trgovčevi banki. Odgovor pošlje ne glede na to, ali dovoljuje transakcijo, ali ne.
7. Trgovčeva banka po opravljeni avtorizaciji pošlje informacijo trgovcu, da je plačilo avtorizirano, ta pa sporoči kupcu, da plačilo sprejema. Pozneje bo trgovec od svoje banke zahteval prenos denarja na njegov račun ali kreditno kartico.
8. Plačevanje preko sistema SET je hitro. Celotna transakcija poteka le nekaj sekund.

Slika 11: Grafični prikaz plačevanja s kreditno kartico preko sistema SET



Vir: http://www.mastercardintl.com/newtechnology/set

[46] virtualna košarica – navidezna oblika nakupovalne košarice, kakršno uporabljamo v klasični trgovini

Prednosti sistema SET

- ***Identifikacija*** – SET s pomočjo digitalnih certifikatov omogoča identifikacijo vseh sodelujočih strank.
- ***Kriptografija*** – SET za varen prenos podatkov uporablja 1024 bitni asimetrični ključ in SSL, ki omogoča vzpostavitev varnega kanala med strežniki in brskalnikom. Uporabljena kriptografija omogoča *avtorizacijo, preverjanje identitete, preprečitev zanikanja transakcije* in *zagotovitev tajnosti*.
- ***Porazdelitev informacij*** – identiteta kupca je delno skrita, saj trgovec lahko razbere le naročilo in način plačila, ne pa tudi identitete kupca. Trgovčeva banka pa dobi le informacije o identiteti kupca, številko kreditne kartice in vrednost nakupa, ne dobi pa informacije o vsebini naročila.

Velik problem SET-a je bila začetna nekompatibilnost programske in strojne opreme različnih dobaviteljev, katera je onemogočala vzpostavitev varnega omrežja s storitvami plačevanja z uporabo protokola SET (Get SET, 2002).

4.1.2. 3D-SET (Three Domain Model)

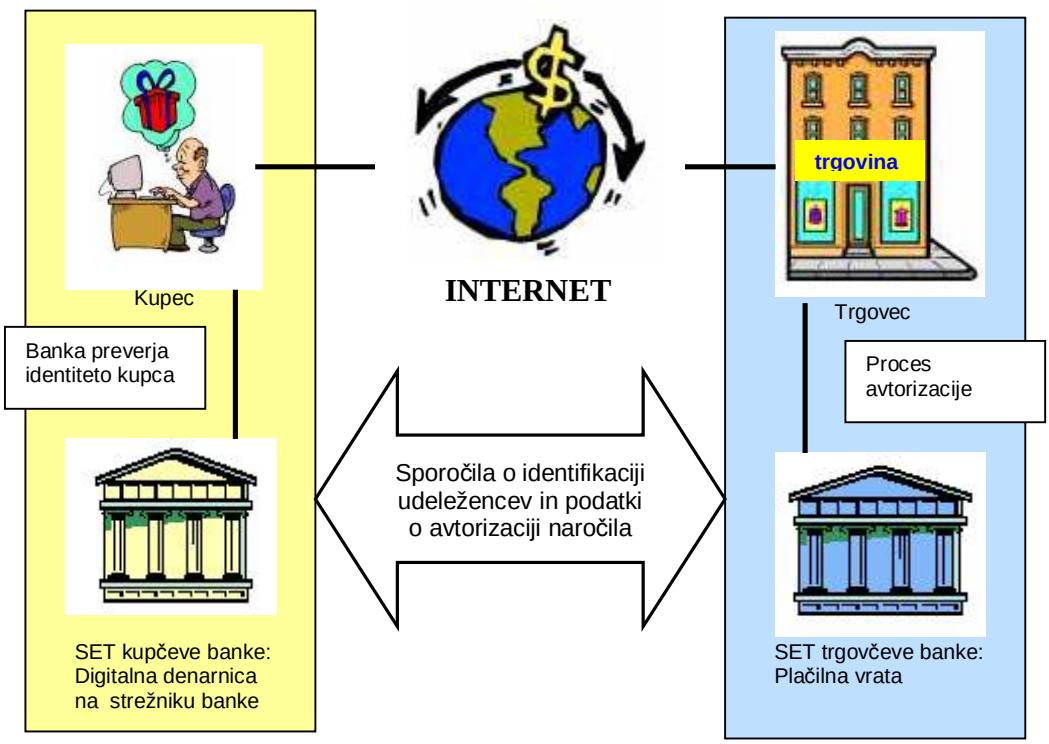
3D-SET je novejša in fleksibilnejša različica SET-a, ki ga je razvila Visa. Sistem SET temelji na infrastrukturi javnih ključev. Za delovanje uporablja ločene digitalne certifikate za vsakega udeleženca posebej (pri prenosu sporočila se uporabljajo štirje pari ključev), kar se odraža na njegovi kompleksnosti. V sistemu 3D-SET ima kupec vse podatke o svojih karticah, digitalni certifikat in informacije o preteklih transakcijah varno shranjene v digitalni denarnici (server wallet) na posebnem strežniku banke, ki mu je izdala kartico. 3D-SET temelji na treh domenah:

- Domena izdajatelja kartic – sestavljata jo kupec in njegova banka,
- Domena trgovčeve banke – sestavljata jo trgovec in njegova banka,
- Inter – operativna domena – sestavljata jo kupčeva banka in trgovčeva banka.

Transakcija se prične, ko kupec na strežniku e-trgovine izbere možnost 3D-SET. Trgovčev strežnik pošlje sporočilo kupčevi banki, ta pa kupcu identifikacijski list, kamor mora vpisati uporabniško ime in geslo. Kupčev digitalni certifikat, ki je shranjen v digitalni denarnici na strežniku tako postane aktiven in lahko se začne preverjanje identitete udeležencev. Nadaljevanje transakcije poteka enako kot v navadnem sistemu SET.

Prednost 3D-SET-a je predvsem v njegovi dostopnosti (inter-operativnost), saj ga lahko uporabljaš kjerkoli po svetu, pa pri tem nisi odvisen od domačega računalnika in na njem shranjene digitalne denarnice. 3D-SET je zaradi svoje manjše kompleksnosti hitrejši in zanesljivejši. Zelo pomembna pridobitev tega sistema je tudi neodvisnost od operacijskega in strojnega sistema (3D-SET, 2002; Selling Online For Merchants – 3D-SET, 2002).

Slika 12: Grafični prikaz 3D-SET modela



Vir: http://visaeu.com/virtual_visa/merchants/3dset.html

4.2. Elektronski denar

Za plačevanje dobrin so denar uporabljali že stari Grki. Le-ta še vedno predstavlja najpomembnejše plačilno sredstvo in ima pred drugimi plačilnimi sistemi kar nekaj prednosti:

- visoka likvidnost – *denar je hitro in široko unovčljivo plačilno sredstvo,*
- nizki stroški transakcij – *pri izmenjavi denarja ni potrebna avtorizacija in vzpostavitev komunikacije,*
- anonimnost – *pri plačevanju z denarjem kupec ostane anonimen in ga je na podlagi denarja praktično nemogoče izslediti.*

Elektronski denar (e-kovanci) je pravzaprav le elektronska različica klasičnega denarja, ki povzema njegove lastnosti. Avtor ideje o elektronskem denarju je David Chaum[47]. Danes najbolj znana sistema z elektronskim denarjem sta Ecash podjetja DigiCash[48] in CAFE[49], ki so ga razvili s projektom ESPRIT pod okriljem Evropske unije. Oba sistema temeljita na elektronski denarnici, ki jo ima uporabnik na svojem računalniku.

[47] http://ntrg.cs.tcd.ie/mepeirce/Project/chaum.html (avtobiografija in članki D. Chauma)
[48] http://www.digicash.com
[49] http://www.semper.org/sirene/projects/cafe/index.html

4.2.1. Ecash

Ecash je varen anonimen plačilni sistem za plačevanje na internetu, ki ga je razvilo podjetje DigiCash. V uporabi je od leta 1995, ko je banka Mark Twain iz ZDA začela kot prva poslovati z elektronskim denarjem.

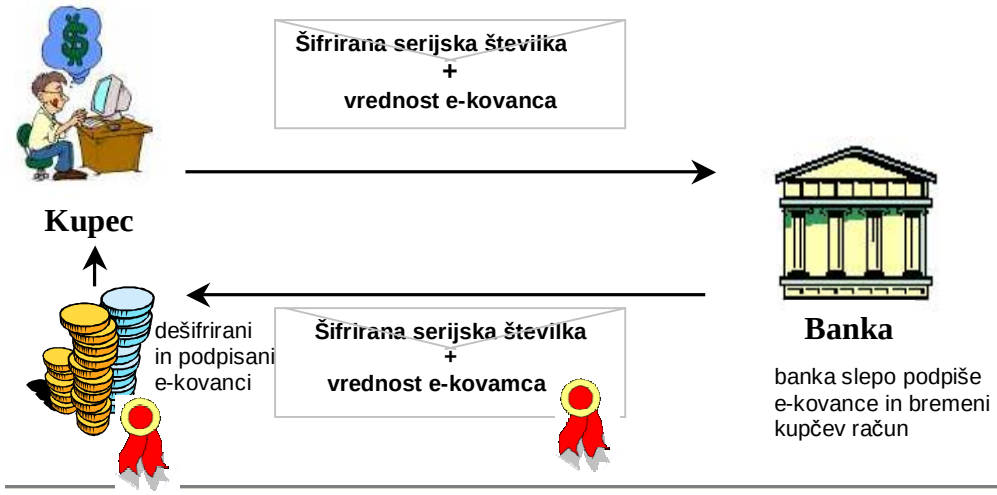
Udeleženci in potrebna orodja v sistemu Ecash

V sistemu elektronskega denarja Ecash so predvideni trije udeleženci: kupec, trgovec in banka, ki podpira sistem Ecash. Pri tej banki morata imeti odprt svoj račun tako kupec kot tudi trgovec. Kupec dviguje elektronski denar pri banki ter ga shranjuje v elektronsko denarnico[50], ki jo ima na svojem računalniku. Elektronska denarnica je programska različica klasične denarnice, v kateri ima kupec shranjene e-kovance, podatke o transakcijah ter varnostne protokole. Banka ob izdaji e-kovancev bremeni kupčev račun za izdano vrednost. Kupec ima tudi možnost pologa e-kovancev nazaj v banko.

Izdaja e-kovancev

E-kovance v sistemu Ecash soustvarja tudi kupec. Za zagotavljanje anonimnosti plačnika je DigiCash vpeljal posebnost, ki se ji reče ***slepi podpis***. Ta omogoča kupcu dvig denarja in pretvorbo le-tega v e-kovance, ne da bi banka lahko pri tem povezala določene kovance z določenim kupcem, kar je lastnost klasične gotovine. Vsak kovanec ima serijsko številko, ki jo generira kupčeva elektronska denarnica. Serijska številka je naključno izbrana številka dolžine 100 cifer, zato je tudi majhna verjetnost njene podvojitve. To serijsko število elektronska denarnica pomnoži s slepilnim faktorjem, ki ga pozna le kupec. Tako šifrirano serijsko številko in vrednost e-kovanca v digitalni kuverti[51] pošlje banki. Banka odšteje vrednost kovanca s kupčevega računa in digitalno podpiše kuverto ter jo vrne v kupčevo digitalno denarnico. Banka z digitalnim podpisom jamči vrednost e-kovanca. Kupčeva elektronska denarnica odstrani digitalno kuverto, šifrirano serijsko številko zdeli s slepilnim faktorjem in tako dobi digitalno podpisan e-kovanec s pravo serijsko številko. Ko je kovanec porabljen, banka ne ve, kdo je oseba, ki ga je porabila, vendar mora izplačati na e-kovancu zapisano vrednost, ker se je s svojim digitalnim podpisom zavezala, da bo to storila.

Slika 13: Potek generiranja e-kovancev z uporabo tehnike slepega podpisa



Vir: O'Mahony, Peirce, Tewari, 2001, str. 146.

[50] program za Ecash poslovanje, ki ga dobi pri banki, v kateri ima odprt račun
[51] digitalna kuverta – elektronska preslikava klasične kuverte

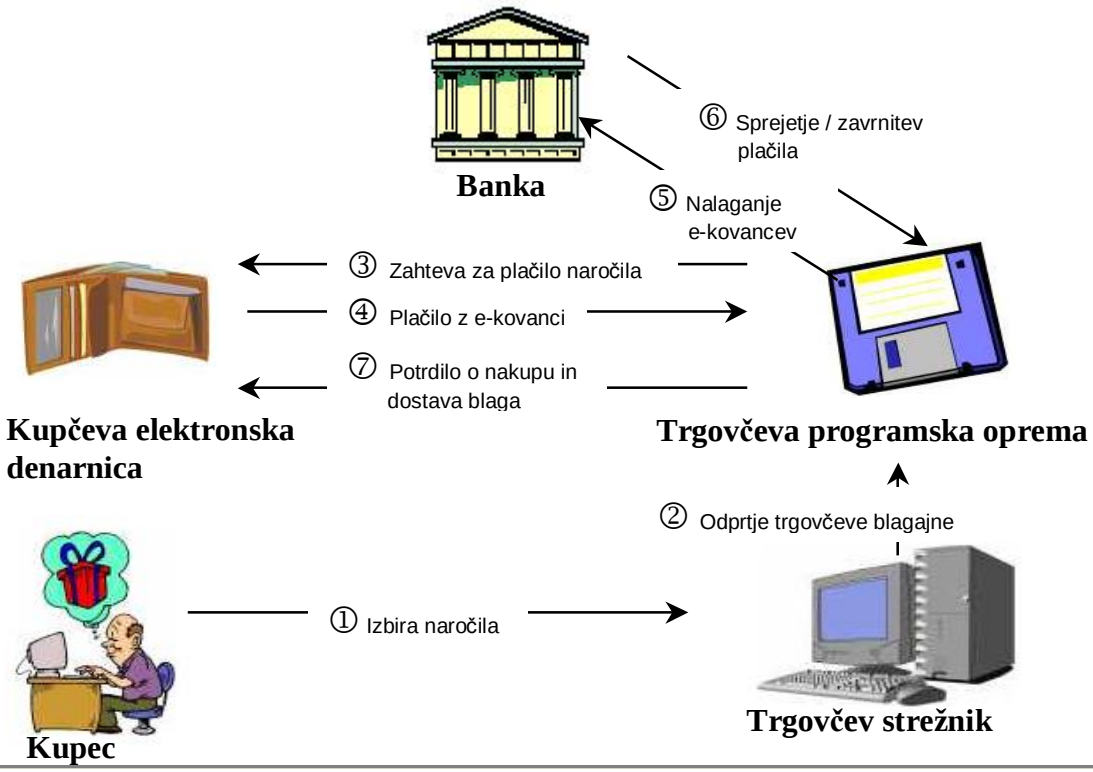
Pri prenosu podatkov Ecash uporablja kombinacijo asimetrične RSA kriptografije in simetrične kriptografije.

Posebnost elektronskega denarja je tudi v tem, da se lahko izdaja v poljubnih vrednostih in ni nujna preslikava denominacije realnega denarja. Tako ni nujno, da so e-kovanci v vrednosti 1 SIT, 2 SIT, 5 SIT, 1000 SIT, temveč so lahko tudi v vrednosti 464 SIT, 12,26 SIT itd.

Potek izvedbe plačila

Kupec z brskalnikom na trgovčevem strežniku izbere blago in trgovcu pošlje naročilo. Trgovec nato pošlje zahtevo za plačilo kupčevi elektronski denarnici. Zahteva za plačilo vsebuje naslednje podatke: valuto, znesek, datum, podatke o banki in bančnem računu trgovca ter opis naročila. Elektronska denarnica kupca vpraša za potrditev plačila. Ob potrditvi plačila elektronska denarnica pošlje e-kovance na trgovčev račun. V primeru, da v denarnici nima drobiža, se elektronska denarnica poveže z banko in opravi zamenjavo. Trgovec te e-kovance posreduje naprej banki, ki preveri njihovo veljavnost. Banka najprej preveri digitalni podpis, s čimer ugotovi, ali je res ona izdajateljica teh e-kovancev. V drugem delu kontrole pa preveri, če ti e-kovanci morda že niso bili kdaj porabljeni. To naredi tako, da serijsko številko e-kovanca primerja z obstoječo bazo že porabljenih e-kovancev. E-kovanci imajo omejeno časovno veljavnost, s katero nekoliko omejimo količino podatkov v bazi že porabljenih e-kovancev. Če serijska številka e-kovanca že obstaja, je bil ta že porabljen. V tem primeru banka ustavi transakcijo in to sporoči trgovcu. V primeru, da serijskih številk ni v bazi že porabljenih e-kovancev, transakcija poteka naprej. Na trgovčevem Ecash računu se poveča vsota za vrednost prejetih e-kovancev, v bazo že porabljenih e-kovancev pa se vpišejo serijske številke le-teh. Trgovec nato pošlje kupčevi elektronski denarnici še potrdilo o nakupu ter dostavi blago (O'Mahony, Peirce, Tewari, 2001, str.146-158).

Slika 14: Poslovanje z elektronskim denarjem Ecash na internetu



Vir: O'Mahony, Peirce, Tewari, 2001, str. 155.

4.3. Sistem aktivnih plačilnih kartic

Sistem aktivnih plačilnih kartic je pravzaprav prenosna elektronska denarnica, ki temelji na tehnologiji pametnih kartic. Elektronski denar se shranjuje v čipu, ki se nahaja na kartici. Na svetu obstaja veliko število med seboj nekompatibilnih aktivnih plačilnih kartic. Najbolj razširjen sistem je Mondex[52], katerega danes uporabljajo v 56. državah. Med pomembnejšimi sistemi so še: nemški GeldKarte[53], finski Avant[54], EMV[55] in Visacash.[56]

4.3.1. Mondex

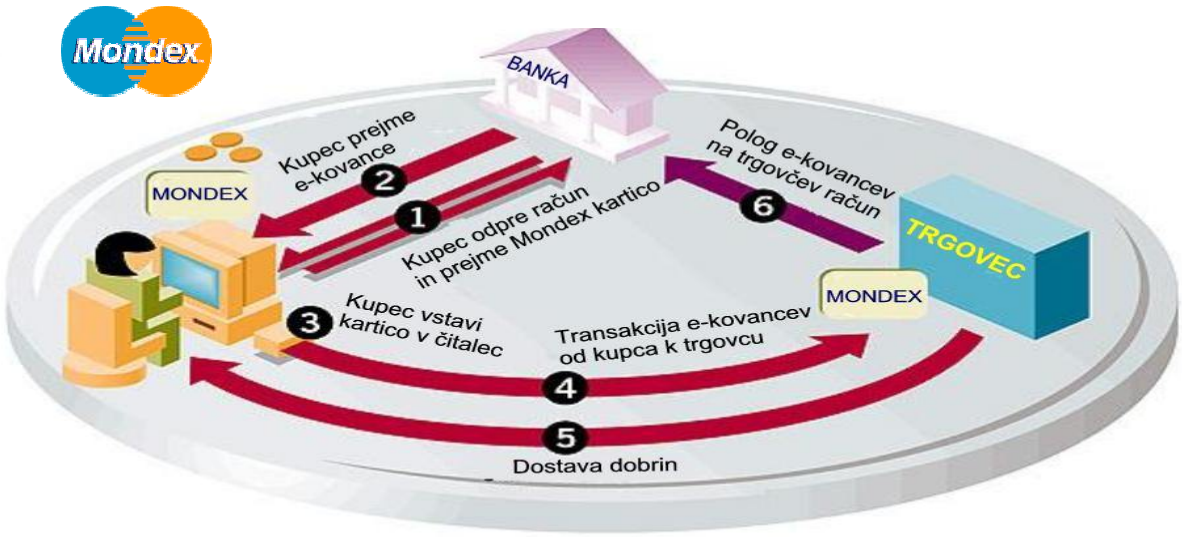
Koncept Mondex je leta 1990 razvila angleška bančna organizacija NatWest v sodelovanju z mnogimi zunanjimi sodelavci. Prva poskusna uporaba Mondexa je bila leta 1992, v katero je bilo vključenih 6000 zaposlenih v NatWestu, ki so lahko v trgovinah in restavracijah znotraj podjetja plačevali z mondexovo kartico. Leta 1995 je prišlo do prve komercialne uporabe, dve leti kasneje pa je večinski lastnik Mondexa postal MasterCard.

Sistem Mondex temelji na tehnologiji pametnih kartic. Njegova pomembna značilnost je omogočanje pretoka e-kovancev iz ene v drugo elektronsko denarnico in obratno, brez vmesnega prenosa e-kovancev v banko, katera podpira sistem Mondex. Sistem Mondex je definiran kot protokol med čipi. Za poslovanje z Mondexovo kartico (polnjenje, plačevanje in ogled stanja sredstev na kartici) so potrebni čitalniki. Čitalniki so različnih oblik in velikosti, od obeska za ključe, ki omogoča le pregled stanja na kartici, oblike žepnega računalnika, ki omogoča prenos e-kovancev z ene kartice na drugo ter čitalniki prilagojeni za delo na osebnem računalniku, telefonu ali mobilnem telefonu. Medij za prenos je lahko internet, telefonska povezava, brezžična povezava ali lokalni čitalnik kartic.

Če želiš postati lastnik Mondexove kartice moraš odpreti račun pri banki, ki podpira sistem Mondex. Banka ti izda kartico in jo napolni z dogovorjeno vsoto e-kovancev, za ta znesek pa ti bremeni račun. Tako kot mnoge druge elektronske denarnice, ki uporabljajo kartico, tudi Mondexova zagotavlja informacije za administracijo poslovanja in podatke o opravljenih informacijah. Tako lahko banka spremlja ves pretok denarja na kupčevem in trgovčevem računu. To omejuje anonimnost sistema, kar mnogi smatrajo kot slabost. Anonimnost plačevanja zagotavlja finska kartica Avant, ki se polni na bančnih avtomatih in je prenosljiva (O'Mahony, Peirce, Tewari, 2001, str. 183-185).

[52] http://www.mondex.com
[53] http://www.geldkarte-trier.de
[54] http://www.avant.fi
[55] http://www.emvco.com (**E**uropay – **M**astercard – **V**isa)
[56] http://www.visacash.com/visacash

Slika 15: Potek nakupa z Mondexovo kartico na internetu



Vir: http://elab.vanderbilt.edu/research/papers/html/student_projects/secure.payment.systems/overview.html

Prednosti uporabe Mondexa (Benefits of Mondex, 2002).

Sistem Mondex prinaša uporabnikom in trgovcem vrsto prednosti:

- Mondex omogoča enostaven prenos denarja med samimi uporabniki in trgovci, brez vmesne avtorizacije v banki.
- Ker pri transakcijah ni potrebne vmesne avtorizacije pri banki, so stroški poslovanja nizki, zato je v nasprotju s kreditnimi karticami zelo primeren za plačevanje majhnih zneskov.
- Tehnično omogoča poslovanje z večjim številom različnih valut naenkrat, kar mu daje internacionalno operativnost. Mondex je edini sistem elektronskega denarja, katerega uporaba je po vsem svetu enaka, zato je primeren za potovanja in transakcije denarja v tujino.
- Sistem Mondex je varen način plačevanja, saj je zasnovan na kriptografiji javnih ključev. Pri uporabi je vedno potrebno vtipkati identifikacijsko številko PIN, kar varuje uporabnika pred nepooblaščeno uporabo.

4.4. Elektronski ček

(O'Mahony, Peirce, Tewari, 2001, str. 125-132; Wade, 1999).
Klasičen papirnati ček je pisni nalog kupčevi banki za prenos sredstev s kupčevega računa na trgovčev račun. Nalog ni poslan neposredno kupčevi banki, temveč trgovcu oziroma prejemniku sredstev. Trgovec oziroma prejemnik mora ček posredovati banki, če želi, da se prenos sredstev izvrši. Ta postopek zahteva visoke stroške transporta čekov in obravnave plačila, poleg tega pa je še zelo počasen.

Ker plačevanje s čeki predstavlja pomemben delež med plačilnimi sistemi, predvsem v ZDA, je konzorcij bank in klirinških hiš FSTC (The Financial Services Technology Consortium) zasnoval eno od različic elektronskega čeka. Podoben sistem je kasneje razvilo tudi podjetje

CyberCash. Z elektronskim čekom sta podjetji FSTC[57] in CyberCash skušala odpraviti pomanjkljivosti klasičnih čekov.

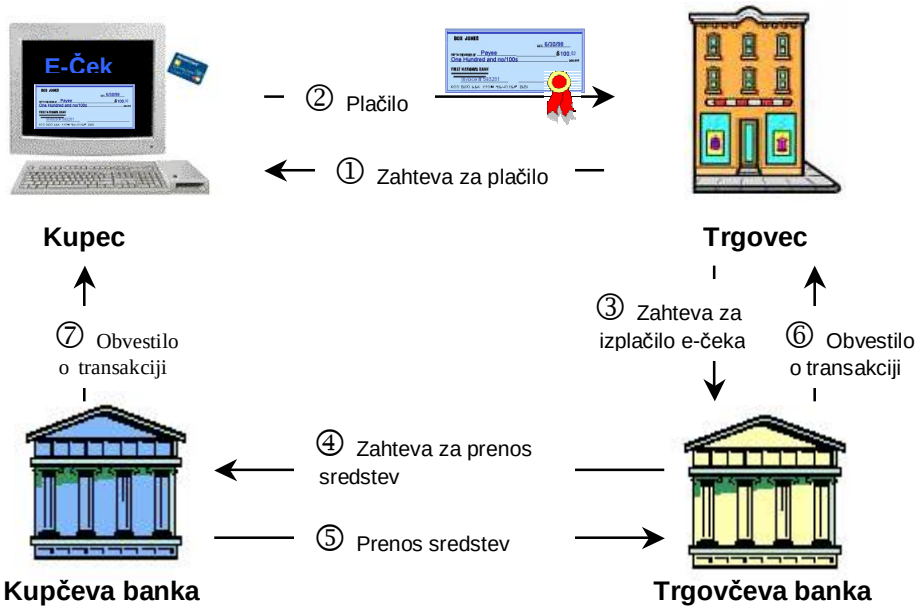
4.4.1. Elektronski ček podjetja FSTC

Elektronski ček ali e-ček je le elektronska različica klasičnega papirnatega čeka. Bistvena razlika je le v tem, da pri e-čeku ves postopek plačevanja poteka v elektronski obliki. Namesto običajnega lastnoročnega podpisa se uporablja digitalni podpis. Sistem FSTC predvideva uporabo pametne kartice, na kateri je shranjena čekovna knjižica. Ta shranjuje podatke o izdanih e-čekih, še ne izdanim določa serijske številke ter jih elektronsko podpisuje. Elektronsko podpisovanje ji omogoča uporabnikov certifikat, ki je tako kot elektronska knjižica shranjen na pametni kartici.

Potek plačila z elektronskim čekom

Plačnik na svojem osebnem računalniku najprej izpolni obrazec e-čeka, nato pa v čitalnik, ki bo s časoma postal sestavni del vsakega računalnika, vstavi pametno kartico. Čekovno knjižico na njej aktivira z vnosom identifikacijske številke PIN. Čekovna knjižica e-čeku določi serijsko številko, ga elektronsko podpiše ter po elektronski pošti pošlje prejemniku. Prejemnik potrdi njegovo prejetje ter ga z zahtevo po izplačilu na njem zapisane vrednosti pošlje svoji banki. Prejemnikova banka nato s plačnikovo banko uredi izplačilo e-čeka ter prenos sredstev s plačnikovega na prejemnikov račun. Na koncu transakcije banki svoja komitenta obvestita o rezultatih izplačila e-čeka.

Slika 16: Potek plačila z elektronskim čekom



Vir: Wade, 1999.

[57] http://www.fstc.org

Sistem FSTC predvideva poleg tega scenarija plačila z e-čekom še možnost, da:

- Plačnik pošlje e-ček prejemniku, ta ga potrdi in neposredno pošlje plačnikovi banki skupaj s svojimi podatki o bančnem računu; banki nato opravita prenos sredstev.
- Plačnik pošlje e-ček neposredno prejemnikovi banki, le-ta pa izda na podlagi e-čeka plačnikovi banki zahtevo za prenos sredstev.
- Plačnik pošlje e-ček svoji banki, s čimer pravzaprav izda nalog za prenos sredstev s svojega na prejemnikov račun.

Do zavrnitve izplačila e-čeka lahko pride zaradi uporabe napačnega ali neveljavnega digitalnega podpisa, kasnejših sprememb na e-čeku (potem, ko je bil ta že digitalno podpisan), ker prejemnik ni znan, ker na bančnem računu plačnika ni dovolj denarja, zaradi napačnega datuma izplačila in izdaje e-čeka v napačni valuti.

Prednosti uporabe elektronskih čekov pred klasičnimi čeki

- mnogo nižji stroški izvedbe transakcije,
- bistveno hitrejši način plačevanja,
- manjša možnost napake,
- udeleženci lahko vedno preverijo verodostojnost podatkov,
- manjša možnost poneverb.

4.5. Sistem mikroplačil

Ti plačilni sistemi omogočajo plačevanje vrednosti blaga in storitev, ki ne presegajo 5 evrov ali 1000 tolarjev. Zelo primerni so za kupovanje programske opreme, glasbe, dokumentov, borznih informacij ter drugih storitev, ki so dosegljive na internetu. Sistemi mikroplačil uporabljajo za plačevanje po internetu enake metode kot drugi elektronski plačilni sistemi. Razlika je le v stroških transakcije. Vrednost teh stroškov ne bi smela presegati vrednosti kupljenega blaga ali storitve, zato ti sistemi vključujejo postopke, ki zagotavljajo manjše stroške za varnost in komunikacijo.

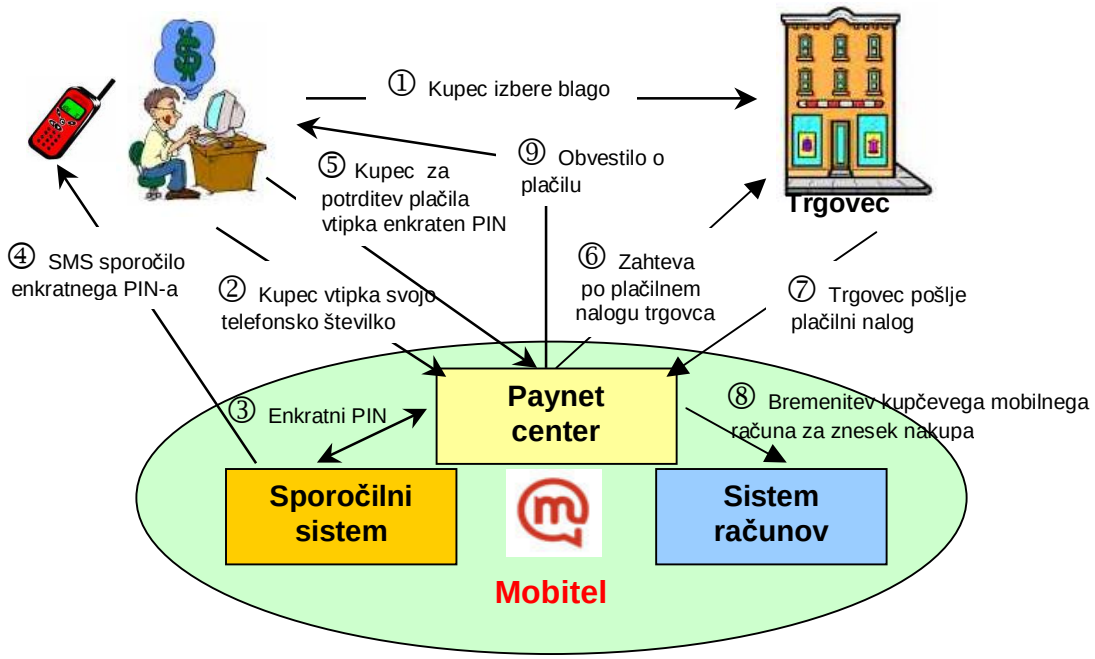
Veliko znanih podjetij je razvilo različne sisteme za mikrotransakcije. V svetu najbolj znan je protokol Millicent, ki ga je razvilo podjetje Compaq/Digital.[58] Sistem Millicent je trenutno v uporabi na Japonskem, kmalu pa bo zaživel tudi v Severni Ameriki in Evropi. V Sloveniji je v uporabi mikroplačilni sistem Paynet[59], ki ga je razvilo slovensko podjetje ADACTA[60].

4.5.1. Paynet

Paynet je mikroplačilni sistem, ki omogoča uporabnikom mobilnih telefonov plačevanje blaga in storitev v mobilnem in fiksnem internetnem okolju. Sistem Paynet, kot storitev pod imenom Moneta[61], ponuja mobilni operater Mobitel. Mobitel je s tem postal prvi evropski ponudnik, ki nudi možnost uporabe mobilnega telefona za plačevanje internetnih storitev. Znesek kupljenega blaga / storitev se prišteje h končnemu računu uporabnika mobilnega telefona. Paynet omogoča poleg mikroplačil tudi plačevanje večjih zneskov.

[58] http://www.millicent.com/home.html
[59] Paynet je svetovna inovacija zaščitena s patentom SLO P-200100103
[60] http://www.adacta.si
[61] http://www.mobitel.si/moneta , http://www.paynet.ws

Slika 17: Potek plačila z mikroplačilnim sistemom Paynet



Vir: Sešek, Olson, 2002, str. 6.

Paynet je enostaven in hkrati zelo učinkovit, varen sistem za plačevanje majhnih zneskov. Varno izmenjavo podatkov med kupčevim računalnikom, trgovčevem strežnikom in Paynet-centrom zagotavlja vzpostavitev varnega kanala SSL. Za potrditev plačila mora kupec vtipkati enkratno PIN kodo, ki jo predhodno preko SMS sporočila prejme od Paynet centra na svoj mobilni telefon. Enkratna PIN koda se lahko uporabi le enkrat, hkrati pa je njeno delovanje tudi časovno omejeno na tri minute in v primeru, da je kupec v tem času ne pošlje nazaj v Paynet center, se proces plačevanja ustavi.

Prednosti uporabe sistema Paynet za kupce in trgovce so predvsem enostavna uporaba, hiter vklop v sistem in varno delovanje, omogoča pa tudi delovanje brez drage dodatne strojne in programske opreme. Kupec ima samo en račun, ki vključuje stroške telefona in stroške nakupa. Mobi uporabnikom je zaradi predplačniškega načina plačevanja zagotovljena tudi anonimnost (Sešek, Olson, 2002, str. 2-18).

4.6. Mobilno plačevanje

Mobilno plačevanje ali m-plačevanje je elektronski način plačevanja s pomočjo mobilnega telefona. Dandanes smo deležni izjemno hitrega razvoja mobilne telefonije. Mobilni telefon že zdavnaj ni več le aparat, namenjen telefoniranju, temveč lahko z njim dostopamo tudi na spletne strani in na njih opravimo nakup. Kljub hitremu razvoju se plačevanje z mobilnimi telefoni še vedno nahaja v zgodnji fazi. To zgodnjo fazo zaznamujejo predvsem različni pristopi izdelave mobilnih telefonov (telefoni z dvema čipnima karticama, telefon prirejen za branje pametnih kreditnih kartic, običajen GSM telefon), uporabe plačilnih instrumentov

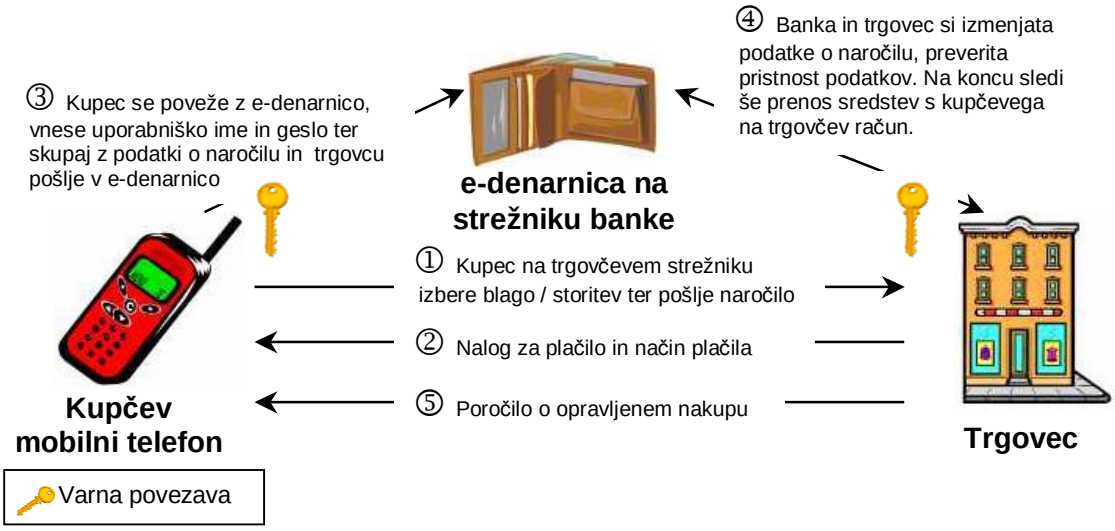
(kreditna kartica, debetna kartica, predplačniška kartica, elektronska denarnica, bančni račun) in njihova operativna funkcionalnost (Krueger, 2002).
Na trgu z m-plačilnimi sistemi že danes vlada velika konkurenca, saj poskusno ali operativno deluje po vsem svetu preko 30 različnih rešitev plačevanja z mobilnimi telefoni. Med vodilnimi podjetji na tem področju je MasterCard. MasterCard je razvil tri sisteme mobilnega plačevanja (E-wallet, 2002):

- plačilni sistem, v katerem z mobilnim telefonom vzpostavimo povezavo z oddaljeno elektronsko denarnico v banki in s pomočjo nje plačamo nakup,
- plačilni sistem, v katerem mobilni telefon opravlja funkcijo čitalnika pametnih kartic,
- plačilni sistem, ki predvideva v notranjosti telefona pametno kartico, na kateri so shranjeni vsi potrebni podatki za izvedbo plačila.

Plačevanje blaga in storitev s pomočjo mobilnega telefona omogoča tudi mikroplačilni sistem Paynet slovenskega podjetja ADACTA. S plačilnim sistemom Paynet lahko plačilo v celoti izpeljemo le z mobilnim telefonom.

V prihodnosti bo m-plačevanje doseglo pomemben delež v elektronskih plačilnih sistemih. Prednost mobilnih plačilnih sistemov je predvsem v tem, da so uporabniku dostopni vsak trenutek, ne glede na to, kje se ta nahaja (na avtobusu, vlaku, restavraciji itd.).

Slika 18: Potek plačila z mobilnim telefonom in elektronsko denarnico



Vir: http://www.mastercardintl.com/newtechnology/mcommerce/whatis/ewallet.html

5. ELEKTRONSKO BANČNIŠTVO

Ko omenimo elektronsko bančništvo, ponavadi pomislimo na storitve, kot so vpogled v stanje računov, plačilo položnic, prenos sredstev med računi in številne druge storitve prek interneta ali mobilnih omrežij. Ena ključnih vlog, ki jih opravljajo banke, je poslovanje z gotovino. Tudi ta se seli v elektronske vode. Prednosti uporabe elektronskega bančništva so:

- nižji stroški transakcij,
- večja hitrost poslovanja,
- vsi podatki so v elektronski obliki in tako lažji za obdelavo,

- manjša možnost napak,
- 24-urna odprtost bančnih poslovalnic,
- opravljanje bančnih storitev brez čakalnih vrst,
- udobnost uporabe za bančne komitente,
- itd.

Napovedi o razvoju e-bančništva so strašljive za tiste, ki niso sledili njegovemu razvoju. Po podatkih znane agencije za trženjske raziskave Gartner Group[62] je on-line storitve leta 1998 ponujalo okoli 1200 bank, ki so predstavljale le 6 % svetovnega bančnega trga, v letu 2000 pa jih je bilo v omrežno bančništvo vključenih že 61 %. Napovedi za leto 2003 kažejo, da bo e-bančništvo ponujalo že 16.000 bank ali tričetrtine svetovnega bančnega trga (Online Banking, 2002).

Slovenija je na področju elektronskega bančništva zelo dobro razvita. E-bančništvo ponujajo vse večje in pomembnejše slovenske banke. Za uspeh pa lahko štejemo, da je večina programskih sistemov e-bančništva v slovenskih bankah plod raziskav in razvoja domačih podjetij, Zaslona d.o.o.[63] (član skupine Hermes SoftLab Group[64]) in ADACTA-e v sodelovanju s tujimi podjetji na tem področju.

Tabela 7: Pregled večjih slovenskih bank, ki ponujajo elektronsko bančništvo

Programska oprema	Banka	Storitev
Družina programov ***Bančni asistent*** podjetja ***Zaslon d.o.o.***	banka celje	banka celje elektronsko bančništvo
	Gorenjska Banka d.d. Kranj	Link
	HYPO ALPE-ADRIA-BANK Slovenija	HYPOnet praktična spletna banka
	ljubljanska banka	klik
	SKB BANKA D.D.	SKB NET
	PBS. Poštna banka Slovenije, d.d.	PBS Pika net
	Nova KBM d.d.	Poslovni Bank@Net
	SLOVENSKA ZADRUŽNA KMETIJSKA BANKA d.d.	sezam
Družina programov ***InetBank*** podjetja ***ADACTA***	ABANKA D.D. LJUBLJANA	ABANET
	Banka	i-Net

Vir: http://www.zaslon.si in http://www.adacta.si

[62] http://www3.gartner.com
[63] http://www.zaslon.si
[64] http://www.hermes-softlab.com

5.1.1. Klik in ProKlik^{+} – e-bančništvo Nove Ljubljanske banke

Nova Ljubljanska banka svojim komitentom ponuja dve različici elektronskega bančništva: Klik in ProKlik plus. Klik pri bančništvu na daljavo uporabljajo občani, medtem ko je ProKlik plus namenjen podjetjem in samostojnim podjetnikom za nemoteno opravljanje elektronskega plačilnega prometa v domovini in s tujino. Za njuno uporabo je potreben račun, ki je odprt pri NLB in ustrezno računalniško opremo.

Storitve, ki jih Klik nudi svojim komitentom

Z nekaj preprostimi kliki z miško lahko kadarkoli in kjerkoli opravimo naslednja bančna opravila:

- vpogled v stanje in promet na svojih računih,
- plačevanje obveznosti in prenose sredstev med računi,
- plačevanje nakupov v spletnih trgovinah,
- naročilo in blokado čekov,
- zahtevek za nakazilo in prevzem gotovine prek sistema Western Union,
- vezavo depozita in prekinitev podaljševanja vezave depozita,
- zahtevek za izdajo in prijavo izgube plačilnih kartic,
- naročilo različnih obrazcev.

Varnost

Uporabnik se identificira s svojim digitalnim certifikatom, ki ga je predhodno pridobil od banke, in osebnim geslom, ki ga pozna samo on. Prav tako se s svojim certifikatom identificira banka. Digitalni certifikat in zasebni ključ se nahajata v obliki datoteke na disku uporabnikovega računalnika, zato moramo preprečiti možnost, da še kdo drug dobi dostop do vsebine te datoteke. Digitalni certifikat in zasebni ključ se lahko hranita tudi na pametni kartici Klik NLB. Uporaba kartice je opcijska in je namenjena predvsem uporabnikom, ki veliko potujejo in gostujejo na različnih računalnikih, iz katerih želijo dostopati do Klika. Za uporabo kartice Klik NLB je potrebna programska oprema Activcard Gold in čitalnik kartice.

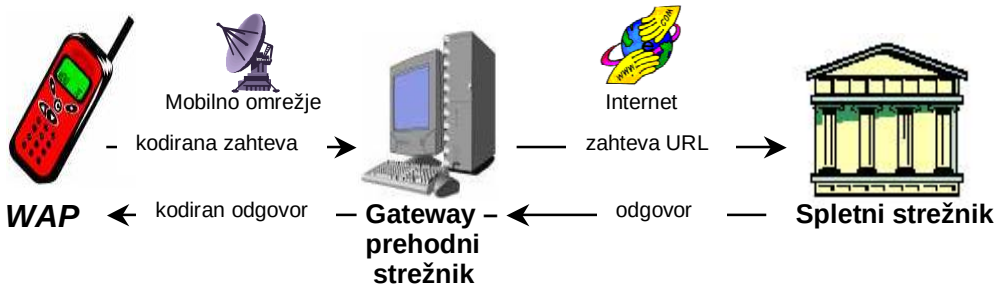
Vsi podatki se prenašajo prek protokola SSL, ta pa jih šifrira s pomočjo 1024 bitnega asimetričnega algoritma RSA in 128 bitnega simetričnega algoritma RC4 (Predstavitev KLIK-a, 2002).

5.1.2. WAP bančništvo

WAP[65] bančništvo ali mobilno bančništvo pomeni selitev storitev, ki jih omogoča e-bančništvo na mobilne telefone. WAP protokol omogoča dostop do spletnih strani s pomočjo mobilnega telefona. WAP bančništvo se danes nahaja v svoji zgodnji fazi in bo v bodoče z razvojem in izboljšavami postalo pomemben člen v poslovanju komitentov s svojimi bankami (glej Sliko 19, str. 38).

[65] WAP (Wireless Application Protocol) – Protokol brezžičnih aplikacij

Slika 19: Mobilna povezava z banko



Vir: Kolar, 2002.

5.1.3. Plačevanje v spletnih trgovinah s Klikom NLB

Nova Ljubljanska banka uporabnikom spletne poslovalnice Klik omogoča varen in preprost način plačevanja spletnih nakupov. Razvili so ga v sodelovanju s podjetjem Zaslon ter spletno trgovino Mladinske knjige, Emka[66]. Trenutno je mogoče prek Klika plačevati le v spletni trgovini Emka, kmalu pa bo to možno tudi v drugih e-trgovinah.

Kupec se na spletni strani trgovca odloči za plačevanje prek Klika, kar pomeni, da se neposredno poveže s svojo spletno bančno poslovalnico. Pred vstopom v Klik se identificira z digitalnim certifikatom in geslom, kar onemogoča morebitne zlorabe računa oziroma nepooblaščen dostop do podatkov uporabnika. Po identifikaciji uporabnik izbere račun, s katerega želi poravnati nakup, in potrdi podatke o plačilu. Prednost plačevanja nakupov v spletni trgovini prek Klika pa je poleg varnega, z digitalnim certifikatom in geslom zaščitenega plačevanja, tudi nižji strošek izvedbe plačila (Koraki nakupa Emka – Klik NLB, 2002).

[66] http://www.emka.si

6. ELEKTRONSKI PLAČILNI SISTEMI V SLOVENIJI

Razmere na področju elektronskih plačilnih sistemov na internetu se tudi v Sloveniji počasi izboljšujejo. Vedno več je podjetij, ki se odločijo za postavitev spletne trgovine. Večina današnjih e-trgovcev omogoča varno plačevanje e-nakupov s kreditno kartico. Načini plačevanja, ki jih naši e-trgovci uporabljajo so še: plačilo po povzetju, plačilo s položnico, plačilo manjših zneskov z Mobitelovo storitvijo Moneta in plačilo prek spletne bančne poslovalnice Klik.

Tabela 8: Večji slovenski spletni trgovci in možni načini plačila e-nakupa

Spletna trgovina	Naslov	Način plačila
DZS	http://www.dzs.si	po povzetju; s položnico; Eurocard, Activa
Emka	http://www.emka.si	po povzetju; s Klikom NLB; Eurocard, Activa
Pasadena	http://www.pasadena.si	po povzetju; s položnico, Visa, American Express, Diners Club, Eurocard / MasterCard
Big Bang	http://www.big-bang-mega.com	po povzetju
Rec Rec	http://www.rec-rec.com	po povzetju
Bofrost	http://www,bofrost-adria.si	po povzetju; Karatnta, Eurocard, Activa
Mercator	http://www.mercator.si	po povzetju z Mercator Pika, Karanto, Eurocard / Mastercardom, Activo, Diners Club, Maestro, BA, Viso, American Express
Merkur	http://nakup.merkur.si	po povzetju; Diners, Eurocard, Activa
ZKP RTV SLO	http://www.rtv.slo/zkpprodaja	po povzetju
Eon	http://www.eon.si/trgovine	po povzetju; Activa, Eurocard / MasterCard, American Express, Visa, Karanta

Vir: Spletne strani slovenskih trgovskih podjetij, 2002.

Z izgradnjo spletne trgovine in kasnejšim zagotavljanjem varnega on-line plačevanja izbranih storitev ali izdelkov s kreditnimi karticami se v Sloveniji ukvarja podjetje Eon[67] d.o.o. Sistemsko rešitev gradi na arhitekturi Transact5 ameriškega podjetja Open Market[68], ki je v svetu največje na tem področju. Eon je pravzaprav posrednik med kupcem, trgovcem in avtorizacijskimi centri. Prednost arhitekture Eona je v prvi vrsti ločevanje vsebine naročila od transakcije (SET) in zagotavljanje visoke varnosti plačevanja. V sodelovanju z Eonom danes posluje preko 40 spletnih trgovin.

Slovenija je zelo dobro razvita na področju elektronskega bančništva, saj skoraj vse slovenske banke ponujajo takšen način poslovanja s svojimi komitenti. Pri elektronskem bančništvu je zelo pomemben podatek, da so programske rešitve e-bank večinoma plod domačega znanja in razvoja v sodelovanju z mednarodnimi podjetji.

[67] http://www.eon.si
[68] http://www.openmarket.com

7. SKLEP

Internet je bil zagotovo ena največjih inovacij devetdesetih let prejšnjega stoletja, njegova priljubljenost in uporabnost pa še vedno strmo naraščata. Kako koristen je lahko internet, se je prepričalo že milijone uporabnikov in le vprašanje časa je, kdaj bo število rednih uporabnikov doseglo milijardo.

Med številnimi revolucionarnimi spremembami, ki jih je internet vnesel v naše življenje, je prav gotovo tudi uvedba elektronskega trgovanja in razvoj elektronskih plačilnih sistemov, kar je bil pogoj za pojav prvih pravih spletnih trgovin. Te si sedaj počasi in zanesljivo utrjujejo položaj enega od glavnih nosilcev globalnega trgovanja.

Spletni trgovci svojim kupcem za plačilo kupljenega blaga omogočajo naslednje možnosti:

- *plačilo po prevzemu,*
- *plačilo s položnico,*
- *plačilo s kreditnimi in debetnimi karticami,*
- *plačilo z elektronskim denarjem,*
- *plačilo z aktivnimi plačilnimi karticami,*
- *plačilo z elektronskim čekom,*
- *plačilo z sistemom mikroplačil,*
- *mobilno plačevanje,*
- *plačilo s pomočjo elektronskega bančništva.*

Vsa plačila, razen plačila po prevzemu in s položnico, so elektronski plačilni sistemi. Prednost varnih elektronskih plačilnih sistemov pred klasičnimi je v nižjih stroških in večji hitrosti upravljanja ter manjši dovzetnosti za napake.

Najpomembnejši elektronski plačilni sistem na internetu je zagotovo kreditna kartica. Resnega e-nakupovanja si ne moremo zamisliti, če nimamo vsaj ene mednarodno priznane bančne plačilne kartice. Izbira ponudnikov je velika, vendar po razširjenosti in uporabnosti izstopata Eurocard / Mastercard in Visa.

Še večjo razširjenost kupovanja v spletnih trgovinah pa zavira strah pred zlorabo kreditne kartice in drugih podatkov. Varnost plačevanja prek interneta je tako predmet mnogih razprav in pogosta tema v medijih. Na podlagi danes dostopne varnostne tehnologije je kupovanje preko interneta varno. Pred nakupom je dobro preveriti varnostno politiko e-trgovca, priporočljivo pa je kupovati pri uveljavljenih in zaupanja vrednih e-trgovcih.

Danes je na svetovnem trgu okoli 150 različnih rešitev internetnih plačilnih sistemov, ki so med seboj povečini nekompatibilni in geografsko omejeni. V prihodnosti bo potrebno doseči vsesplošni dogovor in izoblikovati mednarodne standarde za internetna plačila. Izoblikovanje standardov bo poenotilo plačevanje in s tem povečalo varnost in udobnost e-kupovanja.

8. LITERATURA

1. Bohle Knud, Krueger Malte: Payment Culture Matters – A comparative EU – US perspective on Internet payments. Background Paper No. 4. [URL: http://epso.jrc.es/], 2001.
2. Bartolini Brane: Denar je nekje v omrežju. Moj mikro, Ljubljana, 6.6.2001, str. 54.
3. Bohle Knud: The Potential of Server-based Internet Payment Systems – An attempt to assess the future of Internet payments. Background Paper No. 3. [URL: http://epso.jrc.es/], 2001.
4. Bratož David: Elektronsko bančništvo za pravne osebe. Seminarska naloga. Novo mesto, 2002, 28 str.
5. Carat Gerard, Bohle Knud, Krueger Malte: Electronic Payment Systems – Strategic and Technical Issues. Background Paper No. 1. [URL: http://epso.jrc.es/], 2000.
6. Centeno Clara: Securing Internet Payments – The potential of PKC, PKI and digital signatures. Background Paper No. 6. [URL: http://epso.jrc.es/], 2001.
7. Curtin Matt, Ranum J. Marcus: Internet Firewalls – Frequently Asked Questions. [URL: http://www.interhack.net/pubs/fwfaq/], 2000.
8. Jerman Blažič Borka: Elektronsko poslovanje na internetu. Ljubljana, Gospodarski vestnik, 2001, 207 str.
9. Kodelja Marjan, Banovič Zoran, Okorn Boštjan: Štirje veličastni. Moj mikro, Ljubljana, 6.6.2001, str. 56 - 57.
10. Kolar Boštjan: WAP bančništvo - tehnologija WAP v finančnem sektorju. [URL: http://www.zaslon.si/bancniasistent/izobrazevanje/prezentacije-kazalo.htm], 15.5.2002.
11. Krueger Malte: The Future of M-payments – Business Options and Policy Issues. Background Paper No. 2. [URL: http://epso.jrc.es/], 2001.
12. Newman Simon: Smart cards. B.k.: IST, 1999, 159 str.
13. O'Mahony Donal, Peirce M. A., Tewari Hitesh: Electronic Payment Systems, Second Edition.B.k.: Artech House, 2001, 339 str.
14. Pays Paul-Andre: An intermediation and payment system technology. Computor networks and ISDN systems. Paris, 1996, str. 1197-1206.
15. Sešek Tomaž, Olson Mattias: Paynet – a Simple and Secure Micro Payment System for Fixed and Mobile Internet. Ljubljana, 2002, 18 str.
16. Štrancar Matjaž: Nakupovanje na internetu. Izola: DESK, 2001, 101 str.
17. Wade Chuck: eCheck – An overview and explanation of security measures. [URL: http://www.echeck.org], 1999.
18. Ward Michael: Digital Certificates and Payment Systems. Information Security Technical Report, Vol. 2, No.4. B.k., 1998, str. 23-31.
19. Young Steve, Cris Le Tocq: SET Comperative Performance Analysis. B.k., Gartner Group , 1998, 48 str.
20. Yung Moti, Raihi M. David: E-commerce applications of Smart Cards. Computor networks. New York, 2001, str. 453-472.

9. VIRI

1. 3D-SET. [URL: http://www.visaeu.com/press_media/factsheets/3d_set.html], Visa EU, 22.3.2002.
2. Selling Online For Merchants – 3D-SET. [URL: http://www.visaeu.com/virtual_visa/merchants/3dset.html], Visa EU, 18.3.2002.
3. Bančni asistent. [URL http://www.zaslon.si/bancniasistent/], Zaslon, 15.5.2002.
4. Benefits of Mondex. [URL: http://www.mondex.com], Mondex, 12.5.2002.
5. Digital Certificates. [URL: http://home.netscape.com/security/techbriefs/certificates/index.html], Netscape, 18.3.2002.
6. Europay, MasterCard and Visa to enable Secure Chip Card Payments Over the Internet. [URL: http://www.mastercardintl.com/about/press/pressreleases.cgi?id=259], MasterCard International, 20.3.2002.
7. E-wallet. [URL: http://www.mastercardintl.com/mcommerce/whatis/ewallet.html], MasterCard International, 20.3.2002.
8. Get SET. [URL: http://www.mastercardintl.com/newtechnology/set/], MasterCard International, 16.3.2002.
9. Global eCommerce Report 2001. [URL: http://www.tnsofres.com/freereport.cmf], TNS Interactive, 18.2.2002.
10. Koraki nakupa Emka – Klik NLB. [URL: http://www.emka.si/klik], Emka, 15.5.2002.
11. Nakupovanje. [URL: http://www.ris.org/rezultati/4.htm], RIS, 31.10.2001.
12. Online Banking. [URL: http://www3.gartner.com/init], Gartner Group, 9.2.2002.
13. Online Purchases Statistics. [URL: http://www.epaynews.com/statistics/purchases.html], Epaynews - ePayment Resource Center, 23.1.2002.
14. Online Purchases Revenues 2000 – 2005. [URL: http://www.aquite.com/research], Aquite Research, 16.2.2002.
15. Predstavitev Klik-a. [URL: http://www.nlb.si/klik.n-lb/], NLB, 15.5.2002.
16. Public Key Cryptography Infrastructure. [URL: http://www.baltimore.com/library/pki], Baltimore Learning Center, 18.3.2002.
17. QSI Secura – 3D-SET Edition. [URL: http://www.qsipayments.com/assets/download], 18.4.2002.
18. SET Secure Electronic Transaction Specification. Book 1: Business Description. [URL: http://www.setco.org/download.html], SETco, 1997.
19. The Smart Card. [URL: http://www.mastercardintl.com/newtechnology/smartcards], MasterCard International, 20.3.2002.
20. Understanding PKI. [URL: http://home.netscape.com/security/pki/understanding.html], Netscape, 18.3.2002.