UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

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

INFORMACIJSKI VIDIK REFORME PLAČILNIH SISTEMOV V REPUBLIKI SLOVENIJI

Ljubljana, junij 2002 **PRIMOŽ MARINŠEK**

IZJAVA

Študent Primož Marinšek izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Mojce Indihar Štemberger, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 10.6.2002 Podpis:

Kazalo

Uvod 1
1. Plačilni sistem v Republiki Sloveniji in v državah Evropske Unije 2
1.1. Osnovne značilnosti plačilnih sistemov 2
1.2. Plačilni sistem v državah Evropske Unije 4
1.2.1. Udeleženci v plačilnem sistemu 5
1.2.2. Značilnosti izvajanja plačilnega sistema v državah EU 6
1.2.2.1. Neto poravnava medbančnih plačil 6
1.2.2.2. Bruto poravnava v realnem času 7
1.2.3. Tveganja pri izvajanju plačilnega prometa v državah EU 7
1.3. Stari plačilni sistem v Republiki Sloveniji in primerjava s sistemi v državah EU 8
2. Reforma plačilnega sistema v Republiki Sloveniji 10
2.1. Razlogi za reformo plačilnega sistema 11
2.2. Potek reforme plačilnega sistema 13
3. Informacijski vidik reforme plačilnega sistema v Republiki Sloveniji 16
3.1. Elektronsko poslovanje 16
3.2. Nove bančne tržne poti 18
3.3. Internet 19
3.3.1. Prenos podatkov preko Interneta 20
3.4. Nevarnosti zlorab podatkov pri elektronskem bančništvu preko Interneta 23
4. Tehnološki vidiki zagotavljanja varnega elektronskega bančništva preko Interneta 24
4.1. Šifriranje podatkov 26
4.1.1. Osnovni deli šifriranja podatkov 26
4.1.2. Simetrično šifriranje (šifriranje s tajnim ključem) 29
4.1.3. Asimetrično šifriranje (šifriranje z javnim in zasebnim ključem) 30
4.1.3.1. Prednosti in slabosti asimetričnega šifriranja 31
4.1.3.2. Digitalni certifikat 31
4.1.3.3. Certifikatni uradi – overitelji javnih ključev 32
4.1.4. Zgostitveni algoritmi 33
4.1.5. Digitalni podpis 34
4.2. Metode šifriranja podatkov 35
4.2.1. Šifriranje podatkov z uporabo programske opreme PGP 35
4.2.2. Infrastruktura javnih ključev (PKI) 36
4.2.3. SSL protokol 37
4.3. Načini dokazovanja identitete uporabnikov 39
4.4. Kriteriji za izbiro ponudnika elektronskega bančništva 41
Sklep 43
Literatura 45
Viri 46

Uvod

Slovenski bančni sistem je v dobrem desetletju doživel velike spremembe. V začetku devetdesetih let prejšnjega stoletja je Slovenija iz socialističnega prešla v tržno gospodarstvo, z razpadom nekdanje Jugoslavije pa se je osamosvojila, s čimer je prevzela tudi nadzor nad svojim bančnim sistemom. Nove razmere tržne ekonomije so med drugim prinesle spremenjene zahteve in potrebe na področju storitev plačilnega prometa, za katere obstoječi plačilni sistem ni bil več primeren.

Po starem zakonu o plačilnem prometu je v Sloveniji te storitve opravljala Služba družbenega knjigovodstva (SDK), ki je obenem izvajala tudi nadzor nad družbeno lastnino. Tržno gospodarstvo takšne oblike lastnine ne pozna, zato tudi nadzor nad njo ni več potreben, poleg tega pa je temelj tržnega sistema konkurenca med ponudniki različnih proizvodov in storitev, tako da ni več smiselno, da bi na trgu določenih storitev, ki so povsem komercialne narave, še obstajal monopol. Plačilni sistem je bilo zato potrebno reformirati, da bi ga prilagodili novim razmeram in uskladili s plačilnimi sistemi v drugih tržnih gospodarstvih. Do zaključka reforme je kot naslednica SDK plačilni promet opravljala Agencija za plačilni promet (APP), v reformiranem plačilnem sistemu pa te storitve opravljajo poslovne banke.

Namen te diplomske naloge je prikazati informacijski vidik reforme plačilnih sistemov. Zaradi silovitega razvoja telekomunikacijskih in informacijskih tehnologij je reforma za vse udeležence v tem procesu pomenila več kot le prenos plačilnega prometa iz APP v poslovne banke. Nove tehnologije so omogočile tudi nove elektronske načine opravljanja plačilnega prometa, ki jih je bilo potrebno informacijsko podpreti za zagotovitev ustrezne varnosti elektronskega poslovanja.

V prvem delu najprej prikazujem splošne značilnosti plačilnih sistemov, nato pa značilnosti plačilnih sistemov v državah Evropske unije (EU) in starega plačilnega sistema v Republiki Sloveniji. Predstavljeni so udeleženci v plačilnem sistemu, sistemi medbančnih poravnav in razlike med starim plačilnim sistemom v Republiki Sloveniji ter plačilnimi sistemi v državah EU.

V drugem delu opisujem reformo plačilnih sistemov v Republiki Sloveniji. Najprej sem navedel glavne razloge in cilje reforme, nato pa sam potek le-te. Projekt reforme se je začel leta 1992 z oblikovanjem predlogov o novem plačilnem sistemu in nadaljeval leta 1994 z oblikovanjem projektne skupine pri Banki Slovenije. Projektna skupina je leta 1996 predstavil strategijo reforme v šestih fazah, ki jo je podprla tudi vlada. Reforma se je začela leta 1997 in naj bi po prvotnih načrtih trajala do leta 1999, vendar se projekt zaradi različnih razlogov zaključuje šele letos.

V tretjem delu predstavljam informacijski vidik reforme plačilnih sistemov in nove bančne tržne poti. Poslovne banke so sočasno z izvajanjem reforme razvile tudi storitve elektronskega bančništva, tako da so podjetja s prenosom plačilnega prometa v banke pridobila tudi možnost hitrejšega in racionalnejšega elektronskega poslovanja preko Interneta. Nov medij pa prinaša številne nevarnosti zlorab podatkov, zato je bilo potrebno razviti metode varnega prenosa podatkov ter vzpostaviti zaupanje v varnost elektronskega bančništva.

Varnost lahko zagotavljamo z različnimi metodami, vse bolj pa se uveljavlja »infrastruktura javnih ključev«, ki temelji na digitalnih certifikatih, zasebnih in javnih ključih ter certifikatnih uradih, ki overjajo digitalne certifikate. Nobena od danes uporabljanih metod ne zagotavlja popolne varnosti, vendar lahko z njihovo dosledno uporabo dosežemo zadovoljivo stopnjo zaščite podatkov, ki nam omogoča varno elektronsko poslovanje. V zadnjem delu zato podrobno opisujem tehnološki vidik zagotavljanja varnosti prenosa podatkov preko Interneta s poudarkom na metodah, ki se uporabljajo v elektronskem bančništvu.

1. Plačilni sistem v Republiki Sloveniji in v državah Evropske Unije

Plačilni sistem v Republiki Sloveniji se je do nedavnega precej razlikoval od plačilnih sistemov v EU in drugih sodobnih tržnih gospodarstvih. Slovenija je bila do leta 1991 ena od republik tedanje SFRJ, kjer je bila uzakonjena drugačna družbeno-ekonomska ureditev kot v državah EU, iz česar je izhajal tudi drugačni plačilni sistem.

Plačilni promet je bil v bivši Jugoslaviji dokaj izvirno oblikovan, saj je združeval nekatere lastnosti tržnih gospodarstev in značilnosti ureditev plačilnega prometa v socialističnih državah. Jugoslovanski model plačilnega prometa se je od tržnega razlikoval predvsem po prisili pravnih oseb, da obveznosti poravnavajo na vnaprej predpisani način preko vnaprej določene institucije, medtem ko v tržnih gospodarstvih velja načelo popolne svobode glede načina poravnave obveznosti.

V nadaljevanju bom predstavil glavne značilnosti plačilnih sistemov v Sloveniji in EU in razlike med njimi.

1.1. Osnovne značilnosti plačilnih sistemov

Plačilni sistem sestavljajo institucije, instrumenti in tehnični mehanizmi za prenos sredstev ter pravila, ki oblikujejo odnose v plačilnem sistemu in njegove zakonitosti (Summers, 1994,

str. 29). Osnovna naloga plačilnih sistemov je olajšati poravnavo denarnih obveznosti, ki nastajajo pri poslovanju ekonomskih subjektov, ter zagotoviti varen in učinkovit prenos sredstev (Potrebe po spremembi slovenskega plačilnega sistema, 1994). Plačilni sistem je pomemben del denarnega sistema vsakega gospodarstva, zato je njegova učinkovitost pomembna tako za udeležence na realnih in finančnih trgih kot tudi za centralno banko in državo samo.

Denarne obveznosti lahko poravnavamo na različne načine. Najosnovnejše plačilo se opravi z neposrednim prenosom gotovine med plačnikom in prejemnikom plačila. Takšna plačila se ne evidentirajo znotraj plačilnega sistema, saj se izvajajo brez posredovanja tretjih oseb ali institucij. V okviru plačilnega sistema pa plačnik prenosa sredstev ne opravi neposredno, temveč preko določene finančne institucije. Denarno obveznost lahko poravna z gotovinskim ali negotovinskim plačilom.

Tako za razvita tržna gospodarstva kot za nekdanje socialistične države je značilno, da je tudi do 80 odstotkov vseh transakcij opravljenih z gotovinskimi vplačili in izplačili (neposredni prenos gotovine brez posredništva finančnih institucij, vplačilo gotovine na račun, dvig gotovine z računa, prenos gotovine z denarno nakaznico itd.), vendar pa je vrednost teh plačil zelo majhna (Grujakovič, 2002, str. 4). Čim večji je znesek plačila, tem večja je namreč težnja po negotovinskih plačilih z negotovinskimi plačilnimi instrumenti, med katere spadajo kreditna plačila, trajni nalogi, čeki in drugi instrumenti. Osnova plačilnega prometa so zato denarne obveznosti, za katere je dogovorjeno negotovinsko plačilo.

Temeljna načela za sistemsko pomembne plačilne sisteme so med drugimi naslednja (Strokovno posvetovanje Prenos plačilnega prometa na banke in naloge v podjetjih, 2000, str. 8):

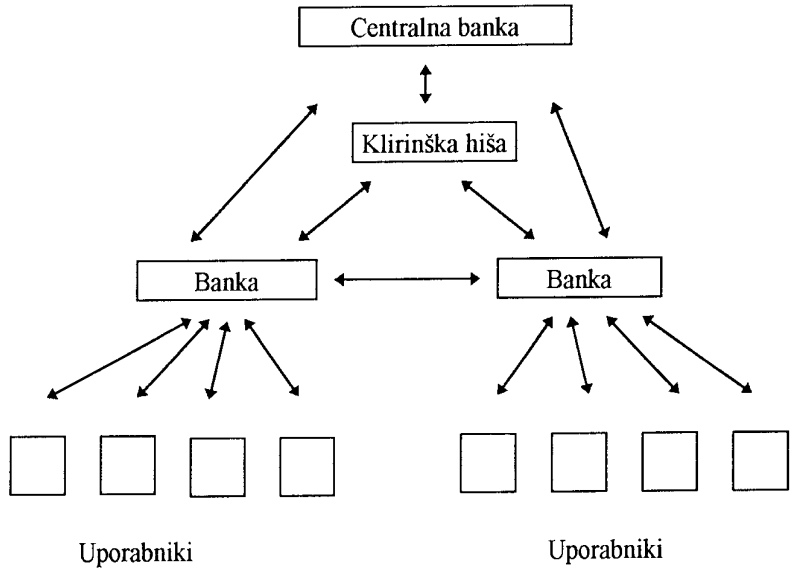
- plačilni sistem mora biti trdno pravno urejen v vseh segmentih pravnega reda;
- pravila in postopki plačilnega sistema morajo omogočati udeležencem jasno razumevanje, kakšnim finančnim tveganjem so izpostavljeni kot udeleženci;
- plačilni sistem mora imeti jasno definirane postopke za obvladovanje kreditnih in likvidnostnih tveganj, tako da so razločno določene odgovornosti nosilca upravljanja plačilnega sistema in udeležencev;
- plačilni sistem mora omogočiti dokončno poravnavo plačil na dan valute;
- v multilateralnem neto plačilnem sistemu mora biti zagotovljen pravočasen zaključek poravnave tudi, če posamezni udeleženec ni sposoben poravnati svoje obveznosti;
- plačilni sistem mora zagotavljati visoko stopnjo varnosti in operativne zanesljivosti in mora predvidevati rezervne rešitve za pravočasni zaključek dnevnih obdelav;
- plačilni sistem mora omogočiti načine plačevanja, ki so praktični za uporabnika in učinkoviti za gospodarstvo;
- upravljanje plačilnega sistema mora biti učinkovito, odgovorno in pregledno.

To so predpisana temeljna načela, ki predstavljajo smernice za opredelitev odgovornosti ter zagotavljanje stabilnosti in varnosti plačilnih sistemov. Veliko vlogo pri zagotavljanju stabilnosti plačilnega sistema ima centralna banka, ki zagotavlja poravnave preko računov, ki jih imajo pri njej poslovne banke, poleg tega pa bankam odobrava kredite, s katerimi zagotovi zadostno likvidnost za nemoteno potekanje plačil.

1.2. Plačilni sistemi v državah Evropske Unije

Plačilni sistemi v državah EU in drugih sodobnih tržnih gospodarstvih imajo običajno obliko piramide, kot je razvidno iz slike 1.

Slika 1: Struktura plačilnega sistema v sodobnih tržnih gospodarstvih



Vir: Potrebe po spremembi slovenskega plačilnega sistema. Banka Slovenije, 1994.

Struktura sistema med drugim poudarja posebno vlogo bank v zagotavljanju plačilnih storitev. Banke imajo vlogo plačilnih posrednikov zato, ker imajo pri njih odprte poravnalne (transakcijske) račune subjekti, ki sodelujejo v ekonomski aktivnosti (Grujakovič, 2002, str. 4). Poleg tega lahko banke s krediti svojim komitentom zagotavljajo likvidnost, ki dovoljuje nemoteno opravljanje transakcij oziroma izvajanje plačilnega prometa. Piramidna struktura poudarja tudi pomembno vlogo centralne banke, ki je na vrhu piramide.

V državah EU je opravljanje plačilnega prometa gospodarska dejavnost, ki jo opravljajo poslovne banke in druge finančne organizacije pod pogoji, ki jih določa zakonodaja posamezne države. Finančne institucije so strogo ločene od nefinančnih, nosilci plačilnega prometa pa so le tiste finančne institucije, ki imajo ustrezno dovoljenje (licenco) in so ustrezno nadzorovane.

1.2.1. Udeleženci v plačilnem sistemu

V procesu negotovinskega plačila denarnih obveznosti v plačilnih sistemih držav EU in drugih tržnih gospodarstvih sodelujejo naslednji udeleženci:

- uporabniki;
- finančne institucije, ki ponujajo storitve plačilnega prometa;
- klirinška hiša;
- centralna banka.

Uporabniki so vsi ekonomski subjekti, ki sodelujejo pri nakupu in prodaji blaga, storitev in drugih oblik premoženja, kjer je dogovorjeno negotovinsko plačilo (Prijanovič, 1997, str. 3). Poleg nefinančnih ekonomskih subjektov (fizičnih in pravnih oseb – podjetij), ki pri takšnih nakupih in prodajah najpogosteje sodelujejo, so uporabniki plačilnega prometa tudi finančne institucije (borzno posredniške hiše, zavarovalnice, investicijski skladi itd), država (oz. državni proračun) in same bančne institucije (banke, hranilnice in kreditne zadruge). Pri vsakem plačilu denarne obveznosti sta vedno prisotna najmanj dva uporabnika (ekonomska subjekta) – plačnik in prejemnik.

Zelo pomembni udeleženci v plačilnem sistemu so finančne institucije, ki ponujajo storitve plačilnega prometa. Plačnik (dolžnik) seveda lahko svojo denarno obveznost poravna z neposrednim (gotovinskim) plačilom prejemniku (upniku). Vendar pa je takšnih plačil relativno malo, saj obstaja veliko število fizičnih in pravnih oseb, ki med seboj poravnavajo različne denarne obveznosti, tako da bi neposredno plačevanje vseh obveznosti ekonomskim subjektom prinašalo le dodatne stroške. Plačnik zato raje opravi vsa svoja plačila na enem mestu - preko določene finančne institucije (poslovne banke). Prav tako prejemnik (ki je seveda lahko v drugih primerih tudi plačnik) raje prejema plačila na enem mestu – npr. preko računa, ki ga odpre pri določeni banki – kot pa, da bi se moral neposredno povezati z vsakim plačnikom posebej. Plačnik in prejemnik imata lahko odprt račun pri isti ali pa pri različnih poslovnih bankah, ki lahko poleg izvajanja storitev plačilnega prometa svojim komitentom omogočijo tudi najemanje kreditov[1] (in s tem lažje poravnavanje denarnih obveznosti) ter investiranje presežnih sredstev.

Klirinška hiša je lahko eden od členov v verigi poravnavanja obveznosti med različnimi bankami. V primeru, da prejemnik in plačnik svojih računov nimata odprtih pri isti banki, mora banka plačnika sredstva v višini plačila prenesti na banko prejemnika. Praksa je pokazala, da je za banke najprimernejši sistem medsebojnega plačevanja prek pobotanja svojih terjatev (Prijanovič, 1997, str. 4). Banke v sodelovanju s centralno banko zato

[1] Kredite lahko uporabnikom ponudijo le kreditne institucije oz. depozitni finančni posredniki, med katere prištevamo poslovne banke, hranilnice in hranilno-kreditne službe. Kreditne institucije se od finančnih ločijo po tem, da javno zbirajo vloge in druge vire nefinančnih ekonomskih subjektov, države in drugih finančnih institucij. S sprejemanjem vlog in dajanjem kreditov kreditne institucije izdajajo knjižni denar, ki postane njihova obveznost. Knjižni denar predstavlja visoko likvidna sredstva, ki se lahko kadarkoli zamenjajo za gotovino, zato se tudi uporablja pri plačevanju (Černuta, 2000).

ponavadi ustanovijo skupno institucijo (klirinško hišo), v kateri se nalogi za plačila zbirajo in obdelajo kot prilivi oz. odlivi na transakcijskih računih bank. Ob koncu poslovnega dne se ugotovijo končna stanja na računih, s tem pa tudi, koliko znašajo terjatve (ali dolgovi) posamezne banke do drugih bank. Plačila med bankami se dokončno poravnajo s sredstvi bank na računih pri centralni banki.

Centralna banka skrbi za nemoten potek plačilnega prometa, v skrajnem primeru pa lahko nastopi tudi kot posojilodajalec, če mora določena banka izvršiti več plačil, kot pa ji dovoljuje stanje na računu pri klirinški hiši. Centralna banka pa ima veliko vlogo tudi na sistemskem področju, saj sodeluje pri oblikovanju pravnega ogrodja za izvajanje plačilnega prometa ter predpisuje pravila delovanja sistema in nadzira njegovo izvajanje (Grujakovič, 2002, str. 43).

1.2.2. Značilnosti izvajanja plačilnega prometa v državah EU

Plačilni promet lahko v okviru posameznega plačilnega sistema razdelimo na notranjega in medbančnega. Notranji plačilni promet se opravlja med poslovnimi partnerji, ki so komitenti iste banke. Plačilne transakcije med komitenti iste banke ne vplivajo na stanje bančnih denarnih sredstev, hitrost v izvajanju plačil v okviru iste banke pa je predvsem odvisna od organizacije plačilnega prometa v banki.

Medbančni plačilni promet se opravlja med komitenti različnih bank. Plačila lahko potekajo neposredno med dvema bankama ali pa preko klirinške (obračunske) hiše. V večini držav EU izvajajo plačila klirinške hiše, ki so ponavadi v lasti poslovnih bank in drugih finančnih institucij ter centralne banke. Klirinške hiše opravljajo obračun (poravnavo) med bankami po načelu neto poravnave medbančnih plačil ali pa po načelu bruto poravnave v realnem času (BPRČ).

1.2.2.1. Neto poravnava medbančnih plačil

Neto poravnava plačil se izvaja za nenujna plačila majhnih vrednosti, ki po številu predstavljajo kar 90 odstotkov vseh plačil, po vrednosti pa le 10 odstotkov celotnega plačilnega prometa (Grujakovič, 2002, str. 21). V sistemu neto poravnav medbančnih plačil klirinška hiša za vsako banko skozi tekoči dan vodi plačila v breme in plačila v dobro njenega transakcijskega računa, nekajkrat dnevno ter po končani dnevni obdelavi pa salde vseh bank med seboj pobota. Prednost neto poravnave medbančnih plačil je predvsem v nižjih stroških takšnega načina poravnave obveznosti, slabost pa v višjem tveganju[2], ki so mu izpostavljeni udeleženci v plačilnem sistemu. Pri pobotanju obveznosti med poslovnimi bankami se namreč lahko izkaže, da katera od bank, ki so udeležene v neto poravnavi, ni zmožna izpolniti svojih obveznosti. V tem primeru mora intervenirati centralna banka, saj bi sicer lahko bil ogrožen celoten sistem neto medbančnih poravnav.

[2] Tveganja pri izvajanju plačilnega prometa opisujem v nadaljevanju.

1.2.2.2. Bruto poravnava v realnem času

Neto poravnava prinaša v plačilni sistem določena tveganja, zato se je v medbančnih plačilih v tržnih gospodarstvih uveljavil sistem BPRČ. Sistemi prenosov sredstev velikih vrednosti so glavne arterije vsakega plačilnega sistema, saj s svojo hitro in zanesljivo poravnavo zagotavljajo varno in učinkovito delovanje denarnih trgov ter trgov kapitala (Grujakovič, 2002, str. 21). Prednost sistema BPRČ je torej njegova zanesljivost, glavna slabost pa višji stroški izvajanja transakcij. Bistvena razlika med sistemoma BPRČ in neto poravnave medbančnih plačil je v času poravnave posamezne transakcije. Medtem ko je v sistemu BPRČ transakcija poravnana takoj (on-line), pa je v sistemu neto poravnave medbančnih plačil dokončna poravnava izvedena šele v okviru neto poravnave med bankami neto dolžnicami in bankami neto upnicami, ki se izvaja nekajkrat v okviru posameznega dneva.

V sistemu BPRČ se plačila poravnavajo posamično (eno za drugim) s knjiženjem v breme banke pošiljateljice in v dobro banke prejemnice in to na njihovih računih pri centralni banki. Prenos denarja je nepreklicen takoj, ko je opravljen, s tem pa je tudi izpolnjena obveznost banke pošiljateljice.

Sistem BPRČ za svoje delovanje zahteva visoko razvit sistem telekomunikacij za elektronsko izmenjavanje sporočil med bankami in klirinško hišo. Zaradi vpliva neposrednih bruto poravnav v realnem času na denarno politiko in njegovih drugih prednosti se je tudi EU odločila uvesti sistem neposrednih bruto poravnav v realnem času za države članice, kar je pomenilo reformo plačilnih sistemov za države, ki so s 1.1.1999 uvedle enotno valuto *euro*. Z uvedbo enotne valute namreč države med seboj ne opravljajo več plačilnega prometa s tujino, temveč domači plačilni promet, zato je bilo potrebno zagotoviti, da so medbančna plačila med komitenti bank držav monetarne unije, ki lahko pomembneje vplivajo na denarno politiko posameznih centralnih bank (oz. evropske centralne banke), izvedena po sistemu BPRČ.

1.2.3. Tveganja pri izvajanju plačilnega prometa v državah EU

Udeleženci v plačilnih sistemih v državah EU so izpostavljeni različnim tveganjem (Grujakovič, 2002, str. 44):

- kreditnemu tveganju;
- likvidnostnem tveganju;
- sistemskem tveganju.

Kreditno in likvidnostno tveganje lahko označimo s skupnim izrazom – poravnalno tveganje, ki izraža verjetnost, da poravnava v plačilnem sistemu ne bo opravljena tako, kot se pričakuje (Pržulj, 2001, str. 4). Do poravnalnega tveganja lahko pride zaradi likvidnostnih motenj ali zaradi plačilne nesposobnosti, omejimo pa ga lahko z izbiro ustreznega sistema za poravnavo plačil. Poravnalno tveganje namreč večinoma izhaja iz časovnih zamikov

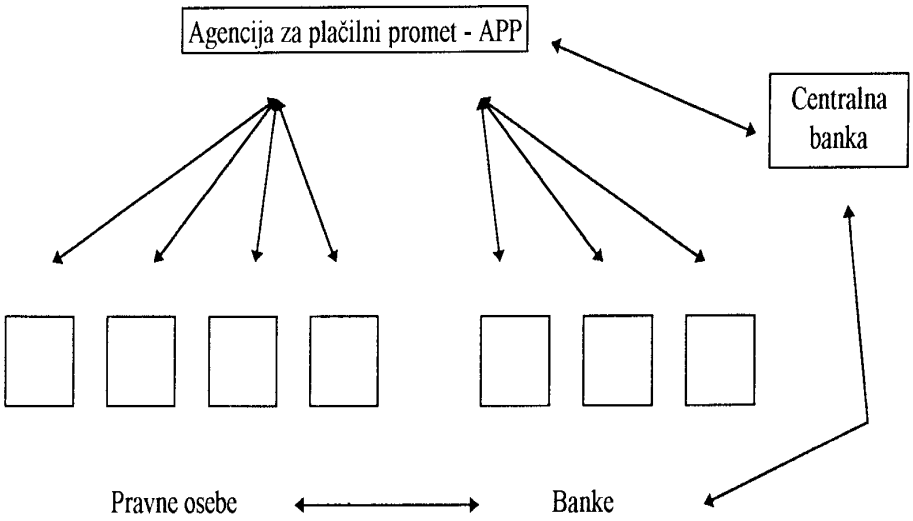
poravnav glede na predložitev plačilnih nalogov. Z uporabo sistema BPRČ so predloženi plačilni nalogi dokončno poravnani takoj, banka pa jih v plačilni sistem lahko posreduje samo, če ima na poravnalnem računu dovolj denarja. Tako je preprečeno kopičenje neporavnanih nalogov, s tem pa se tudi odpravi poravnalno tveganje. Ker pa sistem BPRČ prinaša višje stroške opravljanja transakcij, ga večina držav kombinira z uporabo sistema neto poravnav. Pri tem sistemu je zaradi odložene poravnave medbančnih plačil sicer prisotno poravnalno tveganje, vendar pa se ta sistem uporablja le za plačila manjših vrednosti, za plačevanje velikih zneskov pa sistem BPRČ.

Najnevarnejše tveganje v plačilnem sistemu je sistemsko tveganje, ki ga opredelimo kot verjetnost, da bodo likvidnostne težave ali težave s plačilno nesposobnostjo enega udeleženca plačilnega sistema povzročile razširitev teh težav na druge udeležence in bo tako ogroženo plačevanje v celotnem gospodarstvu (Strokovno posvetovanje Prenos plačilnega prometa na banke in naloge v podjetjih, 2000, str. 9).

1.3. Stari plačilni sistem v Republiki Sloveniji in primerjava s sistemi v državah EU

Slovenija je bila do leta 1991 del nekdanje SFRJ, v kateri je po zakonu iz leta 1962 plačilni promet opravljala SDK. SDK je bila več kot le posrednik denarja, saj je tudi odkrivala in odpravljala deviantna dejanja v družbi (Prijanovič, 1997, str. 11). Njena primarna naloga je bila nadzor družbene lastnine, ki ga je opravljala s kontroliranjem denarnih tokov podjetij, računovodskim revidiranjem in pobiranjem davkov, za potrebe države pa je opravljala tudi različne informacijsko-statistične storitve. Strukturo starega plačilnega sistema v Republiki Sloveniji in vlogo SDK v njem prikazujem v sliki 2.

Slika 2: Struktura starega plačilnega sistema v Republiki Sloveniji



Vir: Potrebe po spremembi slovenskega plačilnega sistema, Banka Slovenije, 1994.

Po prehodu v tržno gospodarstvo vlada ni takoj ukinila SDK, vendar pa se je v Sloveniji začel proces privatizacije družbene lastnine, zato je bilo potrebno preoblikovati tudi službo, ki je opravljala nadzor te lastnine. Leta 1994 je bila SDK z zakonom preoblikovana v Agencijo za plačilni promet, nadziranje in informiranje (APPNI). APPNI je prevzela večino del in nalog SDK v prehodnem obdobju, v katerem naj bi se pripravile podlage za reformi plačilnega in davčnega sistema (Prijanovič, 1997, str. 12). Šele s spremembami zakona o APPNI leta 1996 je Agencija dokončno izgubila svojo nadzorno funkcijo in se preimenovala v APP, še naprej pa je obdržala izključno pristojnost za opravljanje plačilnega prometa za pravne osebe.

APP je opravljala plačilni promet med samimi pravnimi osebami ter med pravnimi in fizičnimi osebami. Pravne osebe so morale imeti svoje račune pri dveh institucijah hkrati, pri banki depozitarju in pri APP, ki je za njih opravljala plačilni promet (Potrebe po spremembi slovenskega plačilnega sistema, 1994). S tem pa so bile prisiljene uporabljati knjižni denar poslovnih bank, ki se ga v tržnih gospodarstvih opredeljuje kot rizičen in zato opcijski denar. Upnik in dolžnik sta v teh sistemih zato svobodna v dogovarjanju, kateri denar bosta uporabila – denar centralne banke (gotovino, ki velja za nerizičen denar) ali knjižni denar poslovnih bank (ki je različno rizičen – odvisno od plačilne sposobnosti posamezne poslovne banke).

Zaradi narave njenega dela nekateri prištevajo APP med finančne institucije, saj je opravljala posel finančnih institucij. Vendar pa je ta posel izvajala na zelo specifičen način, saj so bila podjetja zakonsko prisiljena uporabljati njene storitve, depoziti, ki so jih pravne osebe pri njej imele, pa so bili izključno namenjeni transakcijam (Posel, 1997, str. 8).

Vloga bank v plačilnem prometu je bila omejena na opravljanje plačilnega prometa za fizične osebe (ne glede na to, ali je bil prejemnik fizična ali pravna oseba). Banke so namreč lahko vodile transakcijske račune le za občane, obrtnike in samostojne podjetnike. Za pravne osebe je transakcijske račune vodila APP, po pogodbi med poslovno banko in pravno osebo pa so ta sredstva (na transakcijskem računu pravne osebe pri APP) istočasno bila tudi depozit pri poslovni banki. Takšna ureditev je bankam onemogočala, da bi imele v vsakem trenutku vpogled v svoje likvidnostno stanje.

V tehničnem smislu je bila APP v bistvu klirinška hiša. Plačila med komitenti iste banke je lahko opravila nemudoma, brez vpliva na likvidnost te banke. Do težav pa je prihajalo pri plačevanju med komitenti različnih bank. Neposreden dostop komitentov v plačilni sistem preko APP (ki ni bila bančna, temveč neodvisna institucija) je namreč povzročal, da banke skozi tekoči poslovni dan niso imele informacij o dejanskih prilivih in odlivih na njihovih žiro računih. Ob koncu poslovnega dneva je tako lahko bilo stanje na žiro računih bank tudi negativno. APP je sicer posamezni banki lahko zagotavljala sprotne informacije o kumulativnih odlivih in prilivih z računov pravnih oseb, ki so bili deponenti pri tej banki, vendar zaradi pozne obdelave glavnine plačilnih transakcij ti podatki bankam niso mogli

služiti za pravočasno oceno dejanskega likvidnostnega položaja (Potrebe po spremembi slovenskega plačilnega sistema, 1994).

Čeprav so podjetja bila prepričana, da je plačevanje preko APP brez tveganja, v resnici ni bilo tako, saj je lahko prišlo do primera, da banka nalogodajalca na svojem žiro računu ni imela dovolj sredstev, tako da obveznost dolžnika ni bila poravnana, ne glede na to, ali je bilo na njegovem računu dovolj sredstev za plačilo obveznosti (Posel, 1997, str. 9). V tem primeru si je banka morala sredstva izposoditi na večernem medbančnem denarnem trgu, na katerem so sodelovale poslovne banke in Banka Slovenije (ali pa uporabiti sredstva obvezne rezerve, če jih je imela na razpolago). Če banka ni mogla dobiti kredita od drugih bank, je zaprosila za posojilo pri Banki Slovenije, če pa je bilo zavrnjeno tudi to posojilo, bi v izjemnem primeru lahko nastopil stečaj te banke. V praksi pa je Banka Slovenije v teh primerih morala prisilno izdajati primarni denar za ohranitev stabilnosti plačilnega sistema (Potrebe po spremembi slovenskega plačilnega sistema, 1994), s čimer je bila omejena njena suverenost pri vodenju monetarne politike.

Glavna razlika med starim plačilnim sistemom v Republiki Sloveniji in plačilnimi sistemi v razvitih tržnih gospodarstvih je torej bila v opredelitvi plačilnega prometa kot dejavnosti, ki jo prek monopolne institucije zagotavlja država. V državah EU je plačilni promet ena od številnih komercialnih finančnih storitev, za katere veljajo tržne zakonitosti.

Druga pomembna razlika pa je bila v poslovnem tveganju. V plačilnih sistemih v tržnih gospodarstvih se poslovno tveganje poskuša zmanjšati s kombiniranjem različnih načinov poravnav medbančnih plačil in drugimi ukrepi. Stari plačilni sistem v Republiki Sloveniji pa je tveganja še povečal, namesto da bi jih poskušal zmanjšati (predvsem tveganje, da banka nalogodajalca ne bo mogla izvesti določenega plačila zaradi negativnega stanja na svojem računu). APP je izvajala poravnavo med nalogodajalci po načelu bruto poravnave, zato je bil za nalogodajalce (podjetja in druge pravne osebe) prenos plačila dokončen (torej nepreklicen in brezpogojen) v trenutku, ko so bila sredstva razknjižena z računa plačnika in preknjižena na račun upnika (Posel, 1997, str. 12). Za poslovne banke pa je bilo plačilo dokončno šele po opravljeni medbančni poravnavi ob koncu dneva, v sklopu katere so morale po potrebi najemati tudi kredite za pokrivanje negativnega stanja na svojih žiro računih, saj sprotnega vpogleda v stanje med dnevom niso imele.

2. Reforma plačilnega sistema v Republiki Sloveniji

Plačilni sistem v državah EU opravljajo poslovne banke, ki si pri ponujanju storitev plačilnega prometa komitentom med seboj konkurirajo. Slovenija pa ob spremembi družbeno-ekonomske ureditve v začetku prejšnjega desetletja ni ustrezno spremenila

plačilnega sistema, zato je obstoječi sistem postal neprimeren za nove pogoje poslovanja. V nadaljevanju predstavljam glavne razloge za reformo starega plačilnega sistema in njen potek.

2.1. Razlogi za reformo plačilnega sistema

Razlogov za reformo obstoječega plačilnega sistema v Republiki Sloveniji je bilo veliko, med najvažnejše pa spadajo (Potrebe po spremembi slovenskega plačilnega sistema, 1994):

- odprava monopola pri opravljanju storitev plačilnega prometa;
- združitev različnih plačilnih sistemov;
- odprava prisile pri plačevanju denarnih obveznosti;
- odprava negativnega vpliva obstoječega plačilnega sistema na razvoj finančnih trgov;
- zmanjšanje likvidnostnega, kreditnega in sistemskega tveganja za uporabnike plačilnega sistema;
- odprava negativnega vpliva plačilnega sistema na monetarno politiko.

Odprava monopola pri opravljanju storitev plačilnega prometa je zelo pomembna, saj v razvitih tržnih gospodarstvih tudi na tem področju vlada konkurenca. Stari plačilni sistem v Republiki Sloveniji je opravljanje plačilnega prometa med pravnimi osebami nalagal APP. APP tako pri opravljanju svojih storitev ni imela konkurence, s tem pa je lahko poljubno oblikovala ceno, hitrost in kvaliteto storitev. Kljub temu, da je z reformo in posodobitvijo lastnega sistema dosegla relativno visoko tehnično učinkovitost, pa njen monopol pri izvajanju teh storitev ni bil več upravičen. Izhajal je iz prejšnjega sistema, ki ni predvideval tržnega gospodarstva in s tem konkurence na vseh področjih, tudi na področju opravljanja storitev plačilnega prometa. Pravne osebe tako niso imele možnosti izbire med npr. cenejšimi in bolj tveganimi načini plačila ter dražjimi, a netveganimi načini plačila (Pržulj, 2001, str. 15).

Slovenska posebnost je bila tudi obstoj več plačilnih sistemov, saj je stara zakonodaja poleg ločitve domačega plačilnega prometa in plačilnega prometa s tujino ločila tudi plačilni promet v domači valuti ter plačilni promet v tuji valuti. Zaradi takšne ločitve sorodnih storitev je podjetje, ki je sicer imelo blokiran žiro račun pri Agenciji za plačilni promet, še vedno lahko upravljalo s sredstvi na svojem deviznem računu, s čimer so se dopuščale različne nepravilnosti. Združitev različnih plačilnih sistemov je bila zato nujna tudi iz vidika preprečevanja gospodarskega kriminala.

V plačilnem sistemu je bilo potrebno odpraviti tudi prisilo pri plačevanju denarnih obveznosti. Značilnost tržnih gospodarstev je svoboda ekonomskih subjektov pri sprejemanju poslovnih odločitev, poleg tega pa so ekonomski subjekti za svoje poslovne odločitve v celoti odgovorni, zato jim je potrebno omogočiti tudi svobodo odločanja o

načinu poravnave svojih denarnih obveznosti. Po veljavni slovenski zakonodaji pa so pravne osebe morale svoje denarne obveznosti (razen dovoljenih izjem) poravnavati negotovinsko prek žiro računov, ki so jih imele pri Agenciji. Zakonodaja je torej prisiljevala uporabo opcijskega knjižnega denarja namesto bankovcev in kovancev centralne banke, kar ni bilo sprejemljivo.

Eden od ciljev reforme obstoječega plačilnega sistema je bil tudi odpraviti negativni vpliv letega na razvoj finančnih trgov. Brez učinkovitega plačilnega sistema namreč ni učinkovitih finančnih trgov, med katere štejemo trg denarja, trg kapitala in devizni trg. Obstoječi plačilni sistem v Republiki Sloveniji je na finančne trge vplival negativno, saj ni podpiral njihovega hitrega razvoja.

Denarni trg se je razvil iz plačilne funkcije poslovnih bank, ki morajo (podobno kot podjetja in drugi ekonomski subjekti, ki imajo denarne obveznosti) poskrbeti za lastno likvidnost. Če njihovo likvidnost neomejeno zagotavlja centralna banka (kot je bil primer v bančnem sistemu nekdanje SFRJ), je denarni trg pravzaprav nepotreben (Posel, 1997, str. 21). V normalnih bančnih sistemih pa centralna banka opravlja le funkcijo posojilodajalca v skrajni sili, zato je plačilni sistem izrednega pomena, saj mora zagotoviti hiter, zanesljiv in cenovno sprejemljiv prenos sredstev med vsemi ekonomskimi subjekti (tako med nefinančnimi subjekti kot med bankami samimi).

Tudi trg kapitala zahteva varen in zanesljiv plačilni sistem. Moderne korporacije (predvsem delniške družbe) so se razvile šele z razvojem vrednostnih papirjev in njihovo enostavno prenosljivostjo. Finančni sistem je svoj pomen pridobil šele z razvojem ustreznih plačilnih sistemov, torej z razvojem finančnih institucij, ki izvajajo storitve plačilnega prometa.

Denarni in kapitalski trg pa dopolnjuje še tretji segment finančnih trgov – devizni trg, ki se brez podpore ustrezno razvitih plačilnih sistemov nikoli ne bi razvil do sedanjih dimenzij. V času vse večje globalizacije (dnevni obseg mednarodnega plačilnega prometa znaša že več kot 1000 miljard dolarjev) so učinkoviti plačilni sistemi potrebni predvsem zaradi financiranja svetovne trgovine in poslovanja transnacionalnih korporacij (Posel, 1997, str. 21).

Banka Slovenije je poleg že omenjenih ciljev z reformo plačilnega sistema želela odpraviti tudi negativni vpliv plačilnega sistema na monetarno politiko. V normalnih razmerah monetarno politiko vsake države vodi njena centralna banka, ki skrbi za stabilnost nacionalne valute ter za finančno stabilnost v državi (oziroma nemoteno zagotavljanje plačil v državi in s tujino). V modernih sistemih papirne valute, v katerih denar nima lastne vrednosti (kot jo je imel npr. v obdobju zlate valute), sloni finančna stabilnost izključno na zaupanju, ki ga ima javnost v denar kot menjalno in plačilno sredstvo (Posel, 1997, str. 22). Centralna banka mora uravnavati količino denarja v obtoku ter posredno (z zaračunavanjem obresti za posojena sredstva) prisiljevati banke k ustrezni naložbeni politiki. Obstoječi sistem

pa ji je nalagal, da APP avtomatično zagotavlja likvidnost. APP je lahko kreirala denar izven nadzora centralne banke (Banke Slovenije), kar je vplivalo na denarno politiko, za izvajanje in vodenje katere je pristojna izključno centralna banka.

2.2. Potek reforme plačilnega sistema

Kljub prehodu v tržno gospodarstvo je Slovenija na področju reforme plačilnega sistema zaradi različnih razlogov napredovala relativno počasi. Banka Slovenije je potrebe po reformi plačilnega sistema predstavila leta 1992, vendar vodstvo tedanje SDK reforme, ki bi v bistvu pomenila ukinitev te službe, ni podprlo. SDK je namesto reforme izvedla proces tehnične modernizacije izvajanja plačilnega prometa, šele kasnejše vodstvo APP pa je bolj aktivno sodelovalo v reformi.

Banka Slovenije je leta 1994 predstavila projekt reforme plačilnega sistema in k njemu povabila poslovne banke. Projektna skupina je tako leta 1996 izdelala posebno strategijo reforme plačilnega sistema, ki je temeljila na določenih zahtevah in omejitvah. Temeljna zahteva je bila, da reforma ne sme ogroziti nemotenega in kontinuiranega delovanja plačilnega prometa (Strategija migracije plačilnega prometa v projektu reforme, 1996). Poleg tega je bilo tudi v času prehoda potrebno zagotovljati ustrezne statistične in davčne informacije. Proces reforme je moral pripraviti banke na opravljanje plačilnega prometa kot sestavnega in izvedenega dela osnovne bančne funkcije - odobravanja kreditov, upravljanja sredstev itd. V strategiji reforme je bil upoštevan tudi cilj integracije domačega plačilnega prometa s plačilnim prometom s tujino ter želja, da bi se reforma opravila s čim nižjimi stroški ter v skladu s pravno regulativo (Strategija migracije plačilnega prometa v projektu reforme, 1996).

Izvedba reforme plačilnega sistema je bila načrtovana v šestih fazah (Nekaj informacij o reformi PS, 2001):

1) prenos računov obvezne rezerve poslovnih bank v Banko Slovenije;
2) vpeljava sistema bruto poravnave v realnem času (BPRČ) za medbančne transakcije;
3) prevzem plačilnega prometa pravnih oseb s strani poslovnih bank;
4) ukinitev bančnih računov pri APP;
5) prenehanje poslovanja posameznih podružnic Agencije, ki nimajo komitentov;
6) vse banke izvajajo lastni plačilni promet.

V prvi fazi, ki je bila opravljena marca 1997, je Banka Slovenije od APP prevzela račune obvezne rezerve za vse banke oz. finančne institucije, medtem ko so žiro računi bank še naprej ostali v APP. Po končani prvi fazi reforme je za spremembe v breme računa obvezne rezerve in v dobro žiro računa poslovna banka morala predati nalog Banki Slovenije, ki je izvedla transakcijo tako, da je najprej odvzela sredstva na računu obvezne rezerve banke, nato je odobrila prehodni račun, ki ga je imela pri APP, nato pa je v APP poslala nalog za

odobritev žiro računa te banke pri APP. Za spremembe v breme žiro računa in v dobro računa obvezne rezerve je banka - tako kot prej - obvestila APP, po novem pa je APP morala o spremembi na računu obvezne rezerve obvestiti Banko Slovenije.

Teh transakcij je bilo sorazmerno malo (približno 200 na mesec), zato s prvo fazo reforme ni bilo večjih problemov. Banka Slovenije je na ta način pridobila vpogled v transakcije in račune obveznih rezerv. Poleg tega se je na operativno majhnem segmentu (100 računov, malo transakcij) preveril koncept prevzema računov bank v Banki Slovenije.

Druga faza reforme je bila namenjena uvedbi dveh plačilnih podsistemov - sistema BPRČ in sistema neto poravnave oziroma žiro kliringa (ŽK), ki sta bila podlaga za prenos plačilnega prometa iz APP v medbančno okolje. Sistem BPRČ je bil vzpostavljen aprila 1998, sistem žiro kliringa pa oktobra istega leta. V sistemu BPRČ se poravnavajo plačila velikih vrednosti in nujna plačila (nujna plačila opredeli plačnik). Meja med velikimi in malimi plačili se je v poteku reforme zniževala. Ob vzpostavitvi sistema BPRČ je bila postavljena na 3 milijone SIT, sedaj (v letu 2002) pa znaša 2 miljona SIT (Grujakovič, 2002, str. 21).

V tej fazi reforme so poslovne banke z Banko Slovenije preko telekomunikacijske povezave začele izmenjavati naloge za plačila velikih vrednosti in nujnih plačil. Prenos sredstev iz enega na drugi bančni račun pri Banki Slovenije je začel potekati v okviru sistema BPRČ. V tej fazi so se vse banke in tudi Banka Slovenije priključile na SWIFT[3] omrežje, Banka Slovenije pa je začela delovati v vlogi poravnalne hiše. Za vsa medbančna plačila velikih vrednosti je banka preko SWIFT omrežja poslala nalog v BPRČ sistem, kjer se je transakcija izvedla v realnem času. Za vsa ostala plačila pa se je banka še vedno obračala na APP na klasičen način. Tudi plačilni promet med komitenti bank je še naprej potekal preko APP.

V okviru sistema ŽK so poslovne banke začele zbirati plačilne naloge posameznih podjetij in jih v zbirni obliki posredovati Banki Slovenije. Sprva so se nalogi posredovali enkrat dnevno ob zaključku plačilnega dneva, kasneje pa je bilo poravnav v okviru dneva že več.

V tretji, najdaljši fazi, ki je skupaj s četrto in peto fazo reforme še zmeraj v teku, so banke začele s postopnim prevzemom izvajanja domačega plačilnega prometa. Z vidika dejanskih sprememb v poslovanju slovenskih družb je ta faza najpomembnejša.

Prvi cilj Banke Slovenije v tej fazi je bil zagotoviti ustrezno pripravljenost poslovnih bank za vodenje računov pravnih oseb in za opravljanje plačilnega prometa. Plačilni promet naj bi postal le sestavni del širšega spleta storitev, ki jih opravlja posamezna poslovna banka. Zato

[3] SWIFT je mednarodna organizacija, ki je omogočila računalniško izmenjavo podatkov med bankami po vsem svetu. Organizacijo je leta 1973 ustanovilo 250 največjih bank iz Evrope in Severne Amerike, sistem za izmenjavo podatkov pa je bil usposobljen za delovanje leta 1977. Danes v sistemu SWIFT sodeluje več kot 2500 bank (Grujakovič, 2002, str. 11).

je Banka Slovenije junija 1999 začela s t.i. pilotskim usposabljanjem bank (PUB), ki je predvideval postopno vključevanje komitentov v reformiran plačilni promet.

Prvi del pilotskega usposabljanja je z vidika podjetja potekal tako, da je podjetje plačilne naloge pošiljalo hkrati na APP in na poslovno banko, s katero je sklenilo poslovni odnos. V tem delu usposabljanja je poslovna banka naloge obdelala v testnem okolju in jih prek informacijskega sistema Banke Slovenije posredovala APP. Dejanska plačila je izvedla APP sama, tako da je plačilni promet še naprej potekal na enak način kot v starem plačilnem sistemu. Zgodaj naslednji dan je APP poslala rezultate obdelave poslovni banki, ta pa jih je posredovala podjetju. Rezultate obdelave je APP uporabila za primerjavo z rezultati lastne obdelave in s tem za oceno pravilnosti oz. ustreznosti.

Po zaključenem pilotskem usposabljanju pa podjetja svojih plačilnih nalogov niso več pošiljala tako APP kot bankam, temveč le slednjim, kjer so bili obdelani, banke pa so izpeljale plačila v okviru reformiranega plačilnega prometa. Enajstega septembra 2000 je tako prvih pet pravnih oseb preneslo račune iz APP v bančno okolje, s čimer se je uradno začel prenos računov v banke (Pržulj, 2001, str. 22).

Tretja faza reforme, ki je povezana s četrto in peto fazo, še zmeraj ni zaključena, saj do letošnjega leta ni bilo zakona, ki bi podjetja prisilil k prenosu svojih transakcijskih računov iz APP v banke, zato so podjetja, ki ponavadi ne želijo spreminjati ustaljenih načinov poslovanja, tovrstne odločitve sprejemala zelo počasi. Nekatera od njih so kasneje (po tem, ko so že prenesla svoj račun iz APP v poslovno banko) celo ponovno odprla račun pri APP, saj to ni bilo v nasprotju z zakonodajo. Marca letos pa je končno bil sprejet nov zakon o plačilnem prometu, ki podjetjem nalaga, da morajo do 30.6.2002 opraviti prenos svojih računov v poslovne banke, s čimer je postavljen tudi rok zaključka reforme plačilnih sistemov. Do 10. maja letos je svoje račune iz APP v banke preneslo 72 odstotkov pravnih oseb, ki sodijo med tristo pravnih oseb z največjimi prihodki v letu 2000, ter 51 odstotkov velikih in srednjih pravnih oseb (S programom pospeševanja bo odprtih več tisoč računov, 2002). Strokovnjaki pa centralno banko in ostale udeležence v reformi plačilnih sistemov že nekaj časa opozarjajo na probleme v plačilnem prometu, ki se bodo lahko pojavili ob koncu junija, saj mora prenos računov v banke še vedno opraviti več kot deset tisoč podjetij, večina le-teh pa bo želela prenesti račune v zadnjih dneh pred rokom (Kisli zmagovalci plačilne reforme, 2002).

V četrti fazi reforme posamezne banke, ki so prevzele račune vseh svojih komitentov, ukinjajo svoje račune pri APP, saj za njih ni več potrebe. Posamezna poslovna banka tako pridobi popolni nadzor nad sredstvi, s katerimi upravlja, ter združi plačilni promet pravnih in fizičnih oseb.

V peti fazi reforme se ukinjajo podružnice APP, ki ostanejo brez komitentov, v šesti (zadnji) fazi reforme pa bo ukinjena celotna APP, saj bodo vse banke imele lastni plačilni promet.

APP bo prenehala izvajati plačilni promet konec junija 2002, ukinjena pa bo nekaj mesecev kasneje, ko bodo zaključeni vsi administrativni postopki reforme plačilnih sistemov.

3. Informacijski vidik reforme plačilnega sistema v Republiki Sloveniji

Z reformo plačilnih sistemov so slovenske poslovne banke začele opravljati storitve plačilnega prometa tako za fizične kot za pravne osebe, s čimer so poleg novih poslovnih priložnosti naletele tudi na organizacijske in tehnične probleme. Banke so se pri ponudbi svojih storitev namreč soočile z množico novih komitentov, katerim dotedanje tržne poti, preko katerih so banke v začetkih devetdesetih let omogočale dostop do svojih storitev (bančno okence, bančni avtomat, telefaksno sporočanje in telefonski klicni center – teledom), zaradi obsežnosti njihovega poslovanja niso več zadoščale (Sistemi bančništva na daljavo, 2000). Že manjše podjetje namreč v povprečju opravi vsaj desetkrat več transakcij kot fizična oseba, vrednost teh transakcij pa je lahko tudi do stokrat višja, zato je zanj zelo pomemben sprotni vpogled v stanje in takojšnja možnost prenosa sredstev med svojimi računi ter na račune drugih pravnih oseb. Vsak dan, ko podjetje svojih sredstev ne investira, temveč ostanejo neizkoriščena na njegovem transakcijskem računu, pomeni zanj določeno izgubo v višini oportunitetnih stroškov. Banka sredstva na računih komitentov obrestuje po minimalni obrestni meri, zato je na računu najbolje hraniti le toliko sredstev, kolikor jih podjetje potrebuje za zagotavljanje tekoče likvidnosti, vsa ostala sredstva pa takoj vložiti v bolj donosne investicije.

Po drugi strani je sprememba družbenoekonomskega sistema prinesla konkurenco tudi na področje bančnih storitev. Poslovne banke so tako že pred reformo plačilnega prometa začele iskati nove načine za čim večjo racionalizacijo poslovanja, hkrati pa so povečale borbo za ohranitev obstoječih in pridobitev novih komitentov.

Zaradi vseh teh dejavnikov so banke zato kljub siceršnji konzervativnosti relativno hitro razvile nove tržne poti, ki jih je omogočil silovit razvoj informacijskih in komunikacijskih tehnologij v devetdesetih letih. Vse nove tržne poti temeljijo na takšni ali drugačni obliki *elektronskega poslovanja* oz. elektronskega bančništva.

3.1. Elektronsko poslovanje

V literaturi srečamo številne definicije elektronskega poslovanja. Evropska komisija ga je opredelila kot katerokoli obliko poslovne transakcije, v kateri stranke delujejo elektronsko, namesto da bi bile v neposrednem fizičnem stiku (European Comission, 1997, str. 9).

Ključne tehnološke sestavine vsakega elektronskega poslovanja so *računalniki, programska oprema (aplikacije)* in *komunikacijske tehnologije* (Toplišek, 1998, str. 3). Komunikacijske tehnologije določajo način prenosa podatkov, poleg tega pa v veliki meri definirajo tudi strojno in programsko opremo računalnikov, saj morata le-ti podpirati ustrezni način prenosa podatkov.

Napačno pa bi bilo, če bi elektronsko poslovanje poenostavljeno predstavili kot izmenjavo podatkov med dvema računalnikoma. Računalnik je sestavljen iz strojne opreme, operacijskega sistema in različnih aplikacij, kar pa samo po sebi še ne zadostuje za elektronsko poslovanje. Tem sestavinam je potrebno dodati še *organizacijo poslovanja*, saj šele z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema (Toplišek, 1998, str. 3). Pomemben del organizacije poslovanja je tudi *pravna ureditev*, ki običajno izhaja iz klasičnih oblik poslovanja, vsebuje pa dodatne določbe, s katerimi opredeljuje specifičnosti elektronskega poslovanja.

Osnova vsakega elektronskega poslovanja so komunikacijske tehnologije, ki služijo kot transportni sistemi. Njihovo jedro so protokoli (standardi oz. pravila) za prenose sporočil. Eden od najbolj znanih mednarodnih protokolov za prenos podatkov je X.400, ki ga v različnih notranjih omrežjih in javnih telekomunikacijskih storitvah uporabljajo za prenos tekstovne elektronske pošte, pa tudi za prenos strukturiranih podatkov (Toplišek, 1998, str. 7). Zelo razširjena protokola za prenos podatkov sta tudi ANSI X.12, ki ga uporabljajo v Združenih državah Amerike, in UN/EDIFACT, ki se uporablja v Evropi in drugod po svetu. V zadnjih letih pa se za prenos podatkov med oddaljenimi računalniki vedno bolj uporablja Internet.

Po raziskavi Datamonitorja bo elektronsko bančništvo preko Interneta v Evropi v naslednjih letih doživelo izredno rast (povprečno 40 odstotkov povečanje števila uporabnikov letno), saj za leto 2004 napovedujejo že 21 miljonov uporabnikov, še leta 1999 pa so te storitve uporabljali le 4 miljoni Evropejcev. Tolikšna rast števila uporabnikov za banke ne prinaša le novih priložnosti, temveč tudi določene pasti. Vsaka banka bo namreč morala natančno oceniti svoje možnosti za kratkoročno in dolgoročno rast, saj bo na podlagi teh ocen prisiljena ustrezno investirati v strojno in programsko opremo, da bi svojim uporabnikom lahko ponudila kakovostne storitve. Investicije v informacijsko tehnologijo so v evropskih bankah leta 1999 znašale le 362 miljonov dolarjev, za leto 2004 pa strokovnjaki ocenjujejo, da bodo presegle 1,4 miljarde dolarjev (Datamonitor, 2000). Tolikšne naložbe v elektronsko bančništvo bodo zato morale biti zelo premišljene, saj bodo pomenile precejšnji zalogaj za večino manjših in srednjih bank, med katere spadajo tudi vse slovenske poslovne banke. Preobsežne investicije bodo bankam povzročile velike oportunitetne stroške, kar bi lahko vodilo v različne varčevalne ukrepe. Lastniki bank bi lahko takšne stroške uporabili tudi kot razlog za zmanjšanje števila zaposlenih, zamenjave na vodilnih položajih in zmanjšanje investicij slovenskih bank na tuje trge. Po drugi strani pa bi premajhne investicije lahko vodile v neustrezno kakovost storitev (preveliko število uporabnikov je že povzročilo

preobremenjenost spletnih strežnikov največje slovenske banke) ali celo v neustrezno varnost elektronskega poslovanja. Za zagotovitev varnosti poslovanja preko Interneta je namreč med drugim potrebno zagotoviti ustrezne požarne zidove[4] ter zagotoviti podporo infrastrukturi javnih ključev (ki jo podrobneje predstavljam v nadaljevanju). Varčevanje na tem področju je praktično nemogoče, zato vsaka odločitev za manjše investicije v varnost elektronskega poslovanja (npr. v cenejše rešitve) skoraj zagotovo pomeni večje možnosti zlorabe podatkov.

3.2. Nove bančne tržne poti

Večina poslovnih bank v Sloveniji se je odločila, da svojim komitentom ponudi tudi storitve elektronskega bančništva, pri čemer se za prenos podatkov uporablja predvsem Internet. Banke ponujajo naslednje nove tržne poti (Sistemi bančništva na daljavo, 2000):

- spletno bančništvo;
- neposredno računalniško izmenjavo podatkov;
- »off-line« bančništvo na podlagi arhitekture odjemalec strežnik;
- GSM in SMS sporočanje;
- prenosne telefone in WAP;
- informacijske terminale.

Spletno bančništvo pravzaprav pomeni tretji korak t.i. samopostrežnega bančništva, ki se je začelo z bančnimi avtomati v sedemdesetih in nadaljevalo s telefonskim bančništvom v osemdesetih letih prejšnjega stoletja. Po nekaterih izračunih je opravljanje transakcij preko Interneta za banke tudi desetkrat cenejše od klasične transakcije, opravljene na bančnem okencu, in štirikrat cenejše od opravljanja transakcij prek telefonskega bančništva (Sistemi bančništva na daljavo, 2000). Po drugi strani je Internet v zadnjih letih postal izredno popularen in vsesplošno dostopen, tako da se njegovo število uporabnikov strmo povečuje. Priljubljenost novega medija in možnost za občutno racionalizacijo poslovanja sta tako večino bank po svetu in v Sloveniji vodila k ponudbi te nove tržne poti. Ker banke v Sloveniji sredi devetdesetih let še niso izvajale plačilnega prometa za pravne osebe, so spletno bančništvo najprej ponudile fizičnim osebam, kasneje pa so razvile tudi različne rešitve za potrebe podjetij.

Komitenti se iz različnih razlogov lahko odločijo tudi za neposredno računalniško izmenjavo podatkov z banko. Ta tržna pot je namenjena predvsem velikim podjetjem, saj poleg določenih koristi prinaša tudi višje stroške poslovanja. Njena temeljna značilnost je v določitvi izmenjanih podatkov, ne pa toliko v načinu prenosa, ki lahko poteka na različne načine od neposredne telefonske povezave do uporabe sistema X.400.

[4] Požarni zidovi so posebni računalniki, ki uporabnikom Interneta omejujejo dostop do spletnih strežnikov. Uporabniki morajo imeti dostop le do storitev, ki jih podjetje preko strežnika ponuja, ne pa tudi npr. do notranjega omrežja, na katerega je strežnik povezan.

Arhitektura odjemalec strežnik odpravlja temeljno pomanjkljivost spletnega bančništva, ki onemogoča delo v načinu, ko uporabniki niso v živo povezani z bančnim strežnikom (Sistemi bančništva na daljavo, 2000). Namenjena je predvsem manjšim in srednjim podjetjem, saj omogoča večbančno poslovanje (pregled računov podjetja pri različnih bankah) ter pripravo plačilnih nalogov v »off-line« načinu (brez povezave z bančnim strežnikom), poleg tega pa se lahko vse podatke avtomatično prenese v informacijski sistem podjetja, tako da ni potrebe po dvojnem vnosu podatkov in s tem povezanih napak pri vnosu ter izgube časa.

Razmah mobilne telefonije prinaša nove možnosti elektronskega poslovanja tudi preko teh naprav. Banke že sedaj ponujajo sporočanje v obliki kratkih sporočil (SMS), ki pa je zaradi varnostnih omejitev omejeno na pošiljanje podatkov v smeri iz banke proti komitentom. Vsebina sporočil zajema vse najpomembnejše informacije za komitente – spremembe na računih (prilivi, odlivi), stanje itd.

Nekatere banke in mobilni operaterji so pričakovali večji razmah mobilnega bančništva z uveljavitvijo protokola WAP, ki omogoča povezavo mobilnega telefona z Internetom. Vendar pa trenutno obstoječa komunikacijska tehnologija še ne omogoča dovolj hitrega prenosa podatkov, tako da ta način poslovanja ni nikoli prav zaživel. Vendar pa nam glavni slovenski mobilni operater že za naslednje leto obljublja mobilni sistem tretje generacije (UMTS), ki bo omogočal mnogo hitrejše povezave z Internetom, kar bo prav gotovo pripomoglo k večji popularizaciji mobilnega elektronskega poslovanja vseh vrst.

Informacijski bančni terminali pa so pravzaprav posodobljeni bančni avtomati, ki v večjem in sodobno oblikovanem ohišju združujejo računalnik in različne vhodno-izhodne naprave (poleg zaslona, občutljivega na dotik, je možno uporabljati tudi prirejeno tipkovnico in miško), kot sestavni del funkcionalnosti pa vsebujejo spletni vmesnik za elektronsko bančništvo. Takšni informacijski terminali bodo verjetno v nekaj letih zamenjali obstoječe bančne avtomate, ki so po obliki in funkcionalnosti že nekoliko zastareli.

Internet prinaša tako nove priložnosti kot tudi nevarnosti za poslovne banke. Za njihovo razumevanje moramo najprej spoznati osnovne značilnosti novega medija ter način prenosa podatkov preko njega.

3.3. Internet

Internet lahko opredelimo kot omrežje vseh omrežij, sestavljeno iz velikega števila računalnikov, ki so locirani po vsem svetu in so povezani v številna računalniška omrežja, preko Interneta pa so povezani tako, da lahko vsak računalnik po elektronski poti komunicira z vsakim (Hoffman, 1996, str.10). Internet v najširšem pomenu besede zajema številne

strežnike, ki nam ponujajo določene storitve, ter združuje množico uporabnikov Interneta. Glavna prednost Interneta je v njegovi izjemni razširjenosti po vsem razvitem svetu in nizkih stroških uporabe njegovih storitev, med katere spadajo predvsem (Šušteršič, 2001, str. 15):

- uporaba svetovnega spleta (World Wide Web-a, WWW-ja) za objavljanje, iskanje ter prenašanje podatkov. Svetovni splet je najhitreje rastoči del Interneta, sestavlja pa ga množica spletnih strani, ki tvorijo obsežen vir najrazličnejših informacij in podatkov. Spletne strani so običajno napisane v programskem jeziku HTML (Hypertext Markup Language)[5], podatki pa se prenašajo po protokolih HTTP[6] ali HTTPS[7];
- prenos datotek iz drugih računalnikov in strežnikov – poteka preko posebnega protokola (FTP – File Transfer Protocol);
- elektronska pošta – to sicer ni izvirna storitev Interneta, saj jo je možno izvajati tudi v drugih omrežjih, vendar pa je ena od najbolj priljubljenih oblik komuniciranja med uporabniki Interneta.

Uporabnikom Interneta so na voljo tudi druge storitve (npr. »klepetanje« oz. neposredna izmenjava sporočil med dvema ali več uporabniki), ki pa niso neposredno povezane z elektronskim poslovanjem.

3.3.1. Prenos podatkov preko Interneta

Prenos podatkov med dvema uporabnikoma Interneta (npr. med komitentom in banko) ne poteka neposredno (kot je to npr. primer pri opravljanju storitev neposredno preko bančnega okenca), saj računalnika obeh uporabnikov nista neposredno povezana med seboj, temveč se podatki prenašajo po različnih poteh preko enega ali več vmesnih spletnih strežnikov, kot je to prikazano v sliki 1 v prilogi.

Za prenos podatkov se uporablja TCP/IP protokol (Transmission Control Protocol / Internet Protocol), ki omogoča prenos podatkov med dvema računalnika z uporabo več vmesnih strežnikov. Protokol je razdeljen na dva dela: protokol za nadzor prenosa podatkov (TCP) in protokol za usmerjanje podatkov preko Interneta (IP).

---

[5] Spletne strani se od navadnih tekstovnih besedil razlikujejo po tem, da lahko vsebujejo povezave do drugih spletnih strani in dokumentov, poleg tega pa so lahko obogatene s slikami, zvokom in videom. Podatke lahko preko spletnih strani prenašamo s pomočjo obrazcev, ki so objavljeni na določeni spletni strani. Prejemnik podatkov tako pripravi spletno stran z ustreznim obrazcem za vnos podatkov, ki ga pošiljatelj izpolni. Prejemnik mora pri izdelavi obrazca tudi določiti, kam naj se podatki pošljejo. Druga možnost za prenos podatkov preko spletnih strani pa je, da prejemnik na svoji spletni strani pripravi povezavo do aplikacije, ki avtomatično opravi prenos podatkov, kar je posebej primerno za prenos večjih količin podatkov. V tem primeru mora pošiljatelj za uspešen prenos podatkov prav tako imeti ustrezno aplikacijo (ki mu jo lahko predhodno preskrbi prejemnik podatkov) ali pa mora podatke predhodno pripraviti v ustrezni obliki (o kateri se je dogovoril s prejemnikom podatkov).

[6] Protokol HTTP (Hypertext Transfer Protocol) omogoča ne le prenos navadnega tekstovnega besedila, temveč tudi slik, zvoka in videa.

[7] Običajno gre za HTTP protokol z dodatnim protokolom za varen prenos podatkov (S je oznaka za varnost, ang. *secure*) . Varnost prenosa podatkov ponavadi zagotovimo z uporabo protokola SSL, ki ga predstavljam v nadaljevanju.

Osnovno načelo prenosa podatkov preko Interneta je, da se podatki ne prenašajo celovito (v enem kosu), temveč kot »paketi« (Danda, 2001, str. 18). Tako se sporočilo, ki ga želimo prenesti preko Interneta, najprej razbije v več kosov (paketov), nato pa se ti paketi posamično prenesejo do ciljnega računalnika, kjer se spet sestavijo v prvotno sporočilo.

Na ta način lahko preko ene povezave (linije) poteka komunikacija med več uporabniki (računalniki), kar je glavna prednost tega protokola. Klasični način povezave med uporabniki (kot je npr. telefonska povezava) takšnega načina dela ne omogoča, saj mora vsak par uporabnikov, ki želita komunicirati med seboj, uporabljati svojo linijo. Ker pa je vedno na voljo le omejeno število povezav, lahko tak sistem hitro postane preobremenjen.

Da bi si lahko uporabniki (s svojimi računalniki) preko Interneta izmenjevali podatke, mora biti vsak od njih enolično označen. V ta namen se uporabljajo IP naslovi oz. številke. Vsak računalnik, ki je neposredno priključen v Internet, dobi svoj IP naslov, sestavljen iz dvanajstih številk (npr. 193.189.160.170).

Ko se sporočilo, ki ga pošiljamo preko Interneta, razbije v več manjših paketov, se vsak od njih opremi tudi s posebno glavo, ki vsebuje IP naslov pošiljatelja in prejemnika paketa (Danda, 2001, str. 21). Ko paket potuje med računalniki po omrežju, vsak računalnik, ki sprejme paket, najprej preveri IP naslov prejemnika in temu primerno paket usmeri naprej do naslednjega računalnika ali omrežja. Takšnim računalnikom, ki skrbijo za usmerjanje paketov preko Interneta, pravimo *usmerjevalniki* (routerji). Če pa je usmerjevalnik hkrati povezan tudi z določenim internim omrežjem (in imajo torej računalniki v internem omrežju preko tega usmerjevalnika tudi dostop do Interneta), pa takšnemu računalniku pravimo *prehod* (gateway). Usmerjevalniki (ali prehodi) torej sprejemajo pakete, ki se prenašajo preko Interneta, in jih usmerjajo naprej do naslednjih usmerjevalnikov (prehodov), ki so bližje ciljnemu računalniku. Ko paket pride do prehoda, ki je najbližje ciljnemu računalniku, ga prehod izvzame iz Interneta in ga odvisno od povezave s ciljnim računalnikom po lokalnem omrežju ali modemu pošlje do tega računalnika.

Kot sem prikazal na sliki 2 v prilogi, lahko proces prenosa podatkov razdelimo na štiri nivoje (Danda, 2001, str. 20):

- aplikativni nivo (aplikacije, s katerimi uporabniki dostopajo do Internetnih storitev);
- transportni nivo (ustvarjanje in sestavljanje paketov sporočil);
- omrežni nivo (naslavljanje in usmerjanje paketov);
- podatkovni nivo (fizično upravljanje s podatki, ki se prenašajo preko Interneta, ter s strojno opremo, ki je potrebna za prenos podatkov).

TCP/IP protokol se izvaja na dveh od teh nivojev. Proces prenosa podatkov se začne na aplikativnem nivoju, ko uporabnik želi npr. poslati elektronsko sporočilo. Aplikacija, s

katero uporabnik pošilja sporočilo, le-to pošlje do transportnega nivoja, kjer ga TCP protokol razbije v več paketov in jih pošlje do omrežnega nivoja.

Na tem nivoju IP protokol vsakega od paketov pripravi za prenos tako, da jih opremi z glavo, v katero zapiše vse podatke, potrebne za prenos paketa preko Interneta (med drugim tudi IP naslov prejemnika in pošiljatelja). Ko so paketi pripravljeni za prenos, podatkovni nivo opravi še ostale korake, potrebne za prenos paketov preko Interneta (preveri povezavo z Internetom, modem oziroma mrežno kartico, nosilec podatkov računalnika itd).

Paketi se nato pošljejo najbližjemu *usmerjevalniku* oz. *prehodu*, nato pa se preko drugih *usmerjevalnikov* in *prehodov* prenesejo do ciljnega računalnika. Sprejem sporočil (oz. paketov sporočil) poteka v obratnem vrstnem redu. Pakete iz Interneta sprejema podatkovni nivo, ki skrbi za povezavo z Internetom.

Podatkovni nivo vsak sprejeti paket pošlje omrežnemu nivoju protokola. Ta preveri IP naslov paketa in ugotovi, ali je ta računalnik končni prejemnik tega paketa ali ne: če je, paket pošlje transportnemu nivoju, če pa ni, pa paket vrne podatkovnemu nivoju, ki ga usmeri do naslednjega računalnika (*usmerjevalnika* oz. *prehoda*).

Na transportnem nivoju TCP protokol sprejema pakete in iz njih sestavlja sporočilo. Paketi lahko prihajajo v drugačnem vrstnem redu, kakor pa so bili poslani, poleg tega pa se kakšen od njih med prenosom lahko tudi poškoduje ali izgubi. TCP protokol mora zato med sestavljanjem sporočila preveriti, ali so paketi prispeli nepoškodovani. Vsak paket se pred pošiljanjem ustrezno označi, tako da transportni nivo prejemnika natančno ve, kateri del sporočila je prispel, hkrati pa transportnemu nivoju pošiljatelja tudi sproti sporoča dolžino vsakega prispelega paketa, tako da se v primeru poškodbe določenega paketa le-ta pošlje še enkrat.

Ko transportni nivo prejemnika prejme vse pakete, je datoteka pripravljena za uporabo, zato jo TCP protokol pošlje aplikativnemu nivoju, s čimer je prenos podatkov zaključen (Danda, 2001, str. 21).

Iz navedenih značilnosti TCP/IP protokola je razvidno, kako enostavno je zbirati podatke, ki se prenašajo preko Interneta. Vse, kar potrebujemo, je aplikacija, imenovana *opazovalec mreže* (ang. network monitor), ki jo instaliramo na *usmerjevalnik* ali *prehod*. Danes je na Internetu tudi brezplačno možno dobiti množico tovrstnih aplikacij, ki so povsem enostavne za uporabo in jih je možno poganjati tudi iz drugih (oddaljenih) računalnikov.

3.4. Nevarnosti zlorab podatkov pri elektronskem bančništvu preko Interneta

Elektronsko poslovanje danes poteka na številne načine, pri čemer se uporabljajo različni protokoli za prenos podatkov. Največja pozornost potencialnih napadalcev pa je vendarle usmerjena v transakcije, ki se opravljajo preko Interneta. Ta medij uporablja že več kot 400 milijonov uporabnikov po vsem svetu (Computer Industry Almanac, 2001), zato ga vsa večja podjetja izkoriščajo kot dodatno tržno pot za ponudbo svojih proizvodov in storitev. Veliko število uporabnikov, ponudnikov storitev in opravljenih transakcij pa pomeni tudi veliko možnosti za zlorabe podatkov, zato je varnost pri elektronskem poslovanju ključnega pomena.

Dejstvo, da podatki, ki jih pošiljamo preko Interneta, na poti od izvornega do ciljnega računalnika potujejo preko velikega števila vmesnih računalnikov (strežnikov), kjer jih je možno zbirati in pregledovati, je tudi razlog, da se lahko nepooblaščene osebe v prenos podatkov vmešavajo na različne načine (Introduction to Public-Key Cryptography, 2001):

- z vpogledom v podatke;
- s spreminjanjem podatkov med prenosom;
- s prevzemom identitete – nepooblaščena oseba bi se npr. lahko izdajala za komercialni strežnik in bi od uporabnikov sprejemala plačila s kreditnimi karticami, lahko pa bi se izdajala za nekega drugega uporabnika in v njegovem imenu opravljala nakupe ali plačila preko Interneta.

Poleg vmešavanja v prenos podatkov pa lahko nepooblaščene osebe povzročijo poslovno škodo tudi s pošiljanjem virusov in drugih nevarnih programov (npr. črvov) ter z »PUS napadi« (preprečitev uporabe storitev, ang. Denial Of Service Attack). Virus lahko onesposobi žrtvin računalnik, tako da pride do uničenja pomembnih podatkov, še hujši pa so takšni virusi (ali črvi), ki nepooblaščeni osebi omogočijo dostop do podatkov na računalniku žrtve takšnega virusa. »PUS napad« pa je napad na določen strežnik na Internetu, ki ponuja različne storitve (npr. storitve nakupovanja preko Interneta ali pa storitve elektronskega bančništva). Napadalci takšen strežnik zasujejo z velikim številom zahtevkov (npr. stalno povprašujejo po ceni nekega izdelka, se prijavljajo v sistem itd), tako da ga preobremenijo, s tem pa preprečijo, da bi dejanske stranke lahko uporabljale storitve, ki jih strežnik omogoča. Ker pa tovrstno povzročanje škode ne vpliva neposredno na splošno varnost elektronskega poslovanja, ga ne bom podrobneje obravnaval. Preprečimo ga lahko na različne načine: uporabniki Interneta se proti virusom najuspešneje branijo tako, da uporabljajo anti-virusne programe, ne prenašajo sumljivih datotek iz drugih računalnikov in ne odpirajo sumljive elektronske pošte, »PUS napadalce« pa je možno odkriti preko njihovega IP naslova in sodno preganjati, saj imajo danes že skoraj vse razvite države sprejeto zakonodajo, ki opredeljuje tudi tovrstne prekrške.

Uporabniki Interneta so v preteklosti kot glavni razlog, zakaj še ne uporabljajo storitev elektronskega bančništva ali možnosti nakupovanja preko Interneta, navajali prav dvome o varnosti takšnega poslovanja oz. strah, da bi nepooblaščene osebe dobile vpogled v njihove podatke in jih zlorabile v lastne namene (International survey of e-commerce, 2000). Z razvojem tehnologij in postopkov za zagotovitev varnosti elektronskega poslovanja je takšnih dvomov vedno manj, seveda pa morajo ponudniki tovrstnih storitev zagotoviti, da se vsi potrebni postopki tudi dejansko izvajajo, poleg tega pa morajo svojim uporabnikom natančno pojasniti mehanizme zagotavljanja varnosti ter razložiti, kako lahko tudi sami pripomorejo k večji varnosti prenosa svojih podatkov pri opravljanju storitev elektronskega poslovanja.

Da bi lahko uporabljali storitve elektronskega bančništva (in elektronskega poslovanja nasploh), je bilo najprej potrebno zagotoviti varen način prenosa podatkov. Računalniška izmenjava podatkov že sama po sebi zahteva uporabo precej kompleksnih tehnologij, zahteve varnega elektronskega bančništva pa zapletenost postopka prenosa podatkov še dodatno povečajo.

Ker je varnost za elektronsko bančništvo ključnega pomena, bom v nadaljevanju predstavil mehanizme boja proti že navedenim nevarnostim zlorabe podatkov, ki nam grozijo pri elektronskem poslovanju.

4. Tehnološki vidiki zagotavljanja varnega elektronskega bančništva preko Interneta

Za zagotovitev varnega elektronskega bančništva preko Interneta je potrebno preprečiti zlorabe podatkov na strani uporabnikov Interneta, zlorabe podatkov na strani ponudnikov storitev elektronskega bančništva preko Interneta in zlorabe podatkov med njihovim prenosom preko Interneta.

Za preprečevanje zlorab podatkov na strani uporabnikov Interneta smo odgovorni uporabniki sami. Z omejevanjem dostopa do svojega računalnika drugim osebam, uporabe le preverjenih aplikacij, »deskanja« po le zaupanja vrednih spletnih straneh ter uporabo antivirusnih programov in drugih zaščit pred trojanskimi konji, črvi in virusi lahko učinkovito onemogočimo morebitne napadalce.

Po drugi strani pa lahko z deskanjem po najrazličnejših spletnih mestih in s kopiranjem datotek z Interneta, uporabo nepreverjenih aplikacij in različnih računalniških igric, zanemarjanjem redne uporabe in ažuriranja antivirusnih programov ter »posojanja« svojega računalnika drugim osebam (prijateljem, sorodnikom, otrokom…) nehote omogočimo

vpogled v lastne podatke nepooblaščenim osebam. Med drugimi uporabniki našega računalnika se lahko najde oseba, ki jo zanimajo naši podatki ter gesla, ki jih uporabljamo za uporabo storitev elektronskega poslovanja, poleg tega pa lahko z nevarnim ravnanjem omogočimo napadalcem, da si s trojanskimi konji (ali drugimi podobnimi programi) omogočijo dostop do našega računalnika ali pa se vmešajo v prenos podatkov preko Interneta.

Podobno kot uporabniki Interneta morajo za preprečitev morebitnih zlorab podatkov na svoji strani poskrbeti tudi banke kot ponudniki storitev elektronskega bančništva. Seveda morajo le-te v zagotavljanje varnosti investirati mnogo večja sredstva kot navadni uporabniki Interneta, saj so zaradi zbirk podatkov, s katerimi upravljajo, dosti pogosteje tarča napadov kot končni uporabniki. Za ustrezno varnost teh podatkov je potrebna dodatna strojna in programska oprema, med katero spadajo med drugim požarni zidovi, programi za nadzor nastavitev požarnih zidov[8] in antivirusni programi. Poleg tega morajo v aplikacijah, s katerimi izvajajo storitve elektronskega bančništva, dosledno uporabljati metode za zagotavljanje varnega elektronskega bančništva, opisane v nadaljevanju, ter z organizacijskimi predpisi (in tudi fizično, z namestitvijo podatkovnih in aplikacijskih strežnikov v posebne računalniške sobe) omejiti interni dostop do zbirk podatkov o svojih komitentih in njihovih transakcijah. Organizacija poslovanja ponudnikov elektronskega poslovanja je v večini razvitih držav (tudi v Sloveniji) podvržena inšpekcijskim pregledom, tako da so lahko ta podjetja (predvsem to velja za banke in druge finančne institucije) tudi kaznovana, če njihova organizacijska struktura ter interni pravilniki in predpisi dovoljujejo vpogled v zaupne podatke nepooblaščenim osebam znotraj ali izven podjetja.

Zaradi odprte narave Interneta, ki ob svojem nastanku ni bil namenjen komercialni uporabi, prenos podatkov ni samodejno zaščiten pred nepooblaščenimi osebami. Podatke morajo zaščititi uporabniki sami, pri čemer lahko pride do številnih napak, zato so najštevilčnejše prav zlorabe podatkov na njihovi poti od pošiljatelja do prejemnika.

Danes poznamo različne metode zagotavljanja večje varnosti pri prenosu podatkov preko Interneta in elektronskega bančništva nasploh. Najboljša rešitev za preprečevanje vpogleda in spreminjanja podatkov s strani nepooblaščenih oseb je šifriranje podatkov, za boj proti prevzemanju lažne identitete pa obstajajo različni načini dokazovanja identitete uporabnika ali strežnika.

[8] Programi za nadzor nastavitev požarnih zidov skrbijo za kontrolo požarnih zidov. V primeru, da ugotovijo spremembo nastavitev, lahko zahtevajo dodatno identifikacijo administratorja, v kritičnih situacijah pa celo popolnoma preprečijo dostop do spletnih strežnikov, s čimer preprečijo napade nepooblaščenih oseb, ki morajo za dostop do spletnega strežnika najprej onesposobiti požarni zid.

4.1. Šifriranje podatkov

Šifriranje podatkov oz. kriptografijo človeštvo uporablja že tisoče let. Beseda izhaja iz grščine in pomeni "tajno pisanje". S šifriranjem lahko spremenimo sporočilo tako, da ga lahko prebere le oseba, kateri je sporočilo namenjeno, ne pa tudi druge, nepoblaščene osebe (Danda, 2001, str. 41). Šifriranje se je v preteklosti največkrat uporabljalo v vojaške in vladne namene, v zadnjih desetletjih pa se je njegova uporaba razširila tudi na gospodarska področja. S pojavom Interneta je kriptografska veda izjemno pridobila na pomenu, saj se je v elektronskem bančništvu le na ta način možno zaščititi pred zlorabo podatkov, ki preko Interneta sicer potujejo povsem odprto in svobodno.

S šifriranjem podatkov pred njihovim pošiljanjem preko Interneta želimo doseči naslednje cilje (Introduction to Public-Key Cryptography, 2001):

- zaupnost podatkov – sporočilo, ki ga pošiljamo, mora ostati zaupno;
- identifikacijo uporabnikov – pošiljatelj sporočila mora dokazati, da je res tisti, za katerega se izdaja;
- integriteto podatkov – potrebno je zagotoviti, da se sporočilo med prenosom ni spremenilo;
- nezmožnost zanikanja – potrebno je zagotoviti, da oseba, ki je sporočilo poslala, tega kasneje ne more zanikati.

Kot lahko vidimo, je prvim trem ciljem, ki so v bistvu odgovor na nevarnosti, ki obstajajo pri prenosu podatkov preko Interneta, dodan še četrti cilj, ki je zelo pomemben za uveljavitev elektronskega bančništva preko Interneta (in elektronskega poslovanja nasploh). Banke in drugi ponudniki svojih storitev preko Interneta morajo imeti trdne dokaze, s katerimi lahko zavrnejo trditve njihovih strank, da niso naročile izvedbe določenih transakcij (plačila nekega računa, nakupa določenih vrednostnih papirjev itd).

Šele s trdnimi zagotovili, da dosega zgoraj naštete cilje, lahko posamezni ponudnik storitev elektronskega poslovanja preko Interneta računa na zaupanje strank in njihovo uporabo teh storitev.

4.1.1. Osnovni deli šifriranja podatkov

Šifriranje podatkov sestavljajo štirje pomembni deli (Danda, 2001, str. 43):

- osnovno sporočilo,
- šifrirni algoritem,
- šifrirni ključ in
- šifrirano sporočilo.

Osnovno sporočilo je sporočilo pošiljatelja prejemniku v svoji izvirni obliki (pred šifriranjem ali po dešifriranju). *Šifrirni algoritem* je matematična operacija, s katero se šifrira oz. dešifrira sporočilo. *Šifrirni ključ* je enolični nabor znakov (npr. šifra ali geslo), ki ga šifrirni algoritem uporabi pri šifriranju podatkov. Podatki se šifrirajo na podlagi vsebine ključa, tako da vsak unikatni šifrirni ključ podatke tudi unikatno zašifrira. *Šifrirano sporočilo* je rezultat šifriranja osnovnega sporočila. Ob ustreznem šifriranju je šifrirano sporočilo neberljivo za nepooblaščene osebe.

V preteklosti, ko je bilo šifriranje podatkov uporabljano predvsem v vojaške namene, se je tajnost šifriranih podatkov zagotavljalo s tajnostjo tako šifrirnega ključa kot šifrirnega algoritma. Vojska svoje podatke tako varuje še danes, za poslovne namene pa je poleg tajnosti podatkov potrebno zagotoviti še splošno zaupanje v ustreznost izbranih šifrirnih algoritmov. Le-ti morajo zato biti javni, da je omogočeno njihovo preverjanje. Tajnost podatkov zato zagotavljamo s tajnostjo šifrirnega ključa.

Stopnja varnosti takšnega šifriranja podatkov je odvisna od dolžine šifrirnega ključa (kdor želi dešifrirati podatke brez uporabe šifrirnega ključa, mora tak ključ izdelati oz. ugotoviti sam; daljši kot je šifrirni ključ, težje ga je ugotoviti[9]). Glede na razvoj strojne opreme in s tem povezano naraščajočo hitrostjo procesiranja podatkov se v elektronskem bančništvu priporoča uporaba 1024-bitnih šifrirnih ključev, saj je krajše ključe možno ugotoviti že v relativno kratkem času.

Pri šifriranju je pomembno upoštevati tudi, kako je bil implementiran šifrirni algoritem (ali je bil implementiran neokrnjen algoritem ali pa morda le njegov del), ali smo šifrirni ključ generirali z ustreznim generatorjem naključnih števil, ali smo izbrali primerno dolg šifrirni ključ ter ali je bilo opravljeno testiranje in izločitev šibkih ključev, ki bi jih bilo moč hitreje odkriti (zelo pomembno pri nekaterih algoritmih).

Spodaj je predstavljen primer enostavnega šifriranja podatkov v dvojiškem sistemu s funkcijo XOR[10] (Uporaba kriptografije - XOR, 2002):

Osnovno sporočilo: 11010
Šifrirni algoritem: funkcija XOR
Šifrirni ključ: 01110

[9] Primer: če bi za šifrirni ključ uporabljali samo eno številko od 0 do 9, bi nepooblaščena oseba, ki bi želela dešifrirati podatke, morala poizkusiti največ 10-krat, da bi odkrila pravi ključ. Če bi uporabili števila od 0 do 99, bi bilo možnih kombinacij že 100. Danes se največkrat uporablja 512- ali 1024-bitne ključe, kar pomeni, da bi nepoblaščena oseba za razbitje takšnega ključa morala najti pravilno kombinacijo izmed kar 2^{512} oz. 2^{1024} možnosti.

[10] Funkcija XOR (imenovana tudi »ekskluzivni ali«) sešteva dve števili; rezultat seštevanja je 1, če je eden od seštevancev 1, drugi pa 0; v vseh drugih primerih je rezultat seštevanja 0.

Postopek šifriranja je naslednji:

Osnovno sporočilo:	11010
Šifrini ključ:	01110

Šifrirano sporočilo:	10100

Za šifriranje podatkov se najpogosteje uporabljajo naslednje metode šifriranja podatkov (Danda, 2001, str. 45):

- simetrično šifriranje (šifriranje s simetričnim ključem);
- asimetrično šifriranje (šifriranje z javnim in zasebnim ključem);
- zgostitveni algoritmi in
- digitalni podpis.

Za zagotavljanje varnega elektronskega bančništva preko Interneta se uporablja kombinacija teh metod, saj je le tako možno zagotoviti najvišjo stopnjo varnosti poslovanja ob še sprejemljivih stroških šifriranja podatkov[11]. V poslovnem svetu tako šifriranje ocenjujejo s poslovno logiko: šifriranje je smiselno takrat, ko ima potencialni napadalec več stroškov z razbijanjem šifriranega sporočila kot pa bi imel koristi od informacije v sporočilu (Danda, 2001, str. 42).

Kombinacija navedenih metod šifriranja zagotavlja takšno kompleksnost šifriranja, da bi tudi najmočnejši računalnik na svetu potreboval nekaj mesecev za dešifriranje sporočila. Če torej na ta način preko Interneta pošiljamo npr. nasvet prijatelju, naj kupi nek vrednostni papir, smo lahko skoraj prepričani, da ta informacija ne bo prišla v napačne roke tako hitro, da bi si nepooblaščena oseba lahko z njo kaj koristila (nasvet že v nekaj dneh ne bo več imel uporabne vrednosti). Podobno velja za plačevanje računov preko Interneta in druge oblike elektronskega poslovanja, saj bi potencialni napadalec potreboval mesece oz. leta vloženega dela (ob velikem znanju in stroških), preden bi lahko dešifriral naše podatke; da bi od dešifriranega sporočila imel korist, bi zato moral dešifrirati sporočila kakšne večje banke, ne pa posameznega komitenta.

Za elektronsko bančništvo preko Interneta zato takšno šifriranje podatkov povsem zadostuje. V primerih, kjer se zahteva posebna stopnja varnosti, pa se seveda uporabljajo drugačne metode šifriranja podatkov (npr. pri izmenjavi sporočil o izdelavi jedrskega orožja ipd., kjer se zahteva takšno šifriranje podatkov, da bi tudi najmočnejši računalniki na svetu, ki bi bili povezani v mrežo in vzporedno analizirali podatke, potrebovali več let za dešifriranje sporočila), pri čemer so tajni tako šifrirni ključi kot tudi sami šifrirni algoritmi.

[11] Potrebno se je zavedati, da z nobeno strojno opremo, metodo šifriranja ali programsko opremo (in z njihovimi kombinacijami) ne moremo zagotoviti popolne varnosti elektronskega poslovanja preko Interneta. Investicije vanje morajo zato biti premišljene, saj lahko sicer zapravimo veliko sredstev za nedosegljive cilje.

4.1.2. Simetrično šifriranje (šifriranje s tajnim ključem)

Pri simetričnem šifriranju podatkov, ki ga prikazujem na sliki 3 v prilogi, lahko dešifrirni ključ izračunamo iz šifrirnega ključa (in obratno), tako da se pri veliki večini simetričnih algoritmov tako za šifriranje kot za dešifriranje podatkov uporablja kar isti šifrirni ključ[12] (Introduction to Public-Key Cryptography, 2001). Šifrirni ključ mora seveda ostati tajen (znan le pošiljatelju in prejemniku sporočila), zato se ta metoda šifriranja podatkov imenuje tudi **šifriranje s tajnim ključem**.

Takšen način šifriranja je zelo učinkovit, saj so simetrični šifrirni algoritmi zelo hitri in uporabniki zaradi šifriranja oz. dešifriranja podatkov ne izgubijo veliko časa. Simetrični ključ omogoča tudi določeno mero identifikacije uporabnika, ker podatkov, zašifriranih z enim šifrirnim ključem, ni možno dešifrirati z drugim. Tako sta lahko pošiljatelj in prejemnik podatkov prepričana, da komunicirata drug z drugim (ne pa s kakšno tretjo, nepooblaščeno osebo) – seveda le v primeru, da sta vsem nepooblaščenim osebam preprečila dostop do šifrirnega ključa.

Šifriranje s simetričnim ključem pa ima nekaj pomanjkljivosti. Prvi problem pri njegovi uporabi je zagotovitev varnega prenosa šifrirnega ključa med pošiljateljem in prejemnikom (ključ ne sme priti v roke nepooblaščeni osebi), drugi problem pa predstavlja število uporabnikov, ki želijo med seboj komunicirati na ta način (Introduction to Public-Key Cryptography, 2001). Vsak šifrirni ključ, ki ga uporabljajo, mora biti unikaten, kar npr. pomeni, da morata uporabnik *A* in uporabnik *B* za medsebojno komunikacijo uporabljati šifrirni ključ k_1, uporabnik *A* in uporabnik *C* šifrirni ključ k_2, uporabnik *B* in uporabnik *C* pa šifrirni ključ k_3. V nasprotnem primeru ne bi več mogli preprečiti vpogleda v podatke nepooblaščenim osebam: če bi npr. tudi uporabnik *A* in uporabnik *C* uporabljala šifrirni ključ k_1, bi uporabnik *B* lahko dobil vpogled v podatke, ki bi si jih izmenjevala (če bi prestregel njuno komunikacijo), ker pri komunikaciji z uporabnikom *A* prav tako uporablja šifrirni ključ k_1. S številom uporabnikov število potrebnih šifrirnih ključev strmo narašča (po formuli $n.(n-1)/2$, pri čemer je n število uporabnikov). Za tisoč uporabnikov tako potrebujemo že 499500 šifrirnih ključev, administracija tolikšnega števila ključev pa je že skoraj nemogoča.
Za potrebe elektronskega bančništva se uporabljajo predvsem naslednji simetrični algoritmi (Uporaba kriptografije – simetrični algoritmi, 2002):

- DES (Data Encryption Standard) in DEA (Data Encryption Algorithm), ki ju uporablja ameriška vlada;
- trojni DES – algoritem DES, ki ga izvedemo trikrat;
- RC2, RC4, RC5 – se imenujejo po avtorju Ronaldu Rivestu;

[12] Tudi šifriranje s funkcijo XOR, ki sem ga prikazal, spada med metode simetričnega šifriranja podatkov, saj lahko uporabimo isti šifrirni ključ tudi za dešifriranje podatkov.

- IDEA (International Data Encryption Algorithm), ki sta ga razvila James L.Massey in Xuejia Lai.

Zaradi navedenih pomanjkljivosti pa se v elektronskem bančništvu simetrično šifriranje ne uporablja samostojno, temveč v kombinaciji z asimetričnim šifriranjem in zgostitvenimi algoritmi.

4.1.3. Asimetrično šifriranje (šifriranje z javnim in zasebnim ključem)

Pri asimetričnem šifriranju namesto istega ključa za šifriranje in dešifriranje podatkov uporabljamo dva ključa, ki sestavljata unikatni par (Danda, 2001, str. 46). S katerimkoli od njiju lahko zašifriramo sporočilo, vendar pa lahko šifrirano sporočilo dešifriramo le s pripadajočim drugim ključem (sporočila ni mogoče dešifrirati niti s ključem, s katerim smo sporočilo zašifrirali, niti s katerimkoli ključem iz kakšnega drugega para ključev). Primer izmenjave šifriranega sporočila z asimetričnim šifriranjem je prikazan na sliki 4 v prilogi.

Vsak uporabnik dobi en par ključev (Danda, 2001, str. 46). Eden od obeh ključev se imenuje **javni ključ in** kot pove že njegovo ime, je namenjen javni uporabi. Drugi ključ pa se imenuje **zasebni ključ** in ga mora vsak uporabnik skrbno hraniti, saj je njegovo sredstvo identifikacije in mora ostati tajen (v primeru, da Janko pridobi Metkin zasebni ključ, se lahko izdaja zanjo in v njenem imenu šifrira in pošilja sporočila). Ker sporočilo, ki ga želimo poslati določenemu uporabniku, zašifriramo z njegovim javnim ključem, pravimo temu načinu šifriranja tudi *šifriranje z javnim ključem*.

Najbolj znani asimetrični šifrirni algoritmi so med drugimi:
- RSA
- Diffie-Hellman
- ElGamal
- DSS

V zgornjem primeru želi Janko poslati šifrirano sporočilo Metki (Janko je torej pošiljatelj, Metka pa prejemnica sporočila). Janko mora najprej dobiti Metkin javni ključ (pošlje mu ga lahko Metka z e-pošto). Nato uporabi ta javni ključ za šifriranje svojega sporočila in Metki preko Interneta pošlje šifrirano sporočilo. Ko Metka prejme šifrirano sporočilo, ga lahko dešifrira s svojim zasebnim ključem. Če je ustrezno poskrbela za tajnost zasebnega ključa, je lahko prepričana, da je samo ona dešifrirala to sporočilo.

Ko pa želi Metka poslati šifrirano sporočilo Janku, je postopek obrnjen. Metka mora najprej pridobiti Jankov javni ključ, nato z njim zašifrira sporočilo in ga Janku pošlje preko Interneta. Ko Janko prejme šifrirano sporočilo, ga dešifrira z lastnim zasebnim ključem. Metka bi lahko sporočilo dodatno zašifrirala z lastnim zasebnim ključem (potem bi ga Janko

moral dešifrirati tudi z njenim javnim ključem), s čimer bi Janku dokazala, da je sporočilo poslala prav ona. Napačno pa bi bilo, če bi sporočilo, namenjeno le Janku, zašifrirala **samo** z lastnim zasebnim ključem, saj bi v tem primeru vsak, ki bi na Internetu prestregel njeno sporočilo in imel njen javni ključ, lahko dešifriral to sporočilo.

4.1.3.1. Prednosti in slabosti asimetričnega šifriranja

Asimetrično šifriranje odpravlja oba problema simetričnega šifriranja. Ni več potrebe po varnem prenosu šifrirnih ključev med uporabniki, saj ključ, ki mora ostati tajen (zasebni ključ), vsi uporabniki hranijo pri sebi in ga ne pošiljajo preko Interneta, javni ključ pa se (nasprotno kot pri simetričnem šifriranju) lahko svobodno pošilja drugim uporabnikom brez strahu pred zlorabo (zaradi lažjega dostopa do javnih ključev obstajajo celo posebni spletni imeniki javnih ključev). Poleg tega vsak uporabnik Interneta za komunikacijo z vsemi drugimi uporabniki potrebuje samo en par ključev (javni in zasebni ključ), medtem ko pri simetričnem šifriranju vsak par uporabnikov uporablja svoj šifrirni ključ (Danda, 2001, str. 46).

Asimetrično šifriranje ima v primerjavi s simetričnim še dodatno prednost, saj omogoča tudi identifikacijo uporabnikov (Danda, 2001, str. 47). Vsak uporabnik ima svoj zasebni ključ, ki mora ostati tajen in ga ne sme deliti z nikomer drugim (za razliko od simetričnega šifriranja, kjer isti šifrirni ključ uporabljata dva uporabnika). Za dokaz svoje identitete mora uporabnik tako le zašifrirati določeno (lahko tudi nesmiselno) sporočilo s svojim zasebnim ključem (pri tem pa mora tisti, ki želi preveriti identiteto tega uporabnika, seveda imeti njegov javni ključ, da lahko dešifrira to sporočilo).

Poleg navedenih prednosti pa ima tudi asimetrično šifriranje svoje pomanjkljivosti. Glavna med njimi je počasnost šifriranja, saj morajo šifrirni ključi biti zelo kompleksni, zato je potrebno več časa za šifriranje in dešifriranje podatkov (Danda, 2001, str. 47). Prav zato se danes pri zagotavljanju varnega elektronskega bančništva preko Interneta uporablja kombinacija asimetričnega in simetričnega šifriranja.

4.1.3.2. Digitalni certifikat

Digitalni certifikat je digitalni dokument, ki se uporablja za identifikacijo uporabnika, podjetja, organizacije oz. kakšnega drugega subjekta. Podobno kot potni list, osebna izkaznica ali vozniško dovoljenje je tudi digitalni certifikat v vse več državah splošno priznan dokaz o identiteti njegovega lastnika (Introduction to Public-Key Cryptography, 2001).

Digitalni certifikat skupaj z zasebnim in javnim ključem uporabnika tvori unikatno kombinacijo. V njem so zapisani podatki o lastniku zasebnega in javnega ključa, tako da jih lahko preverimo vsakič, ko nas zanima identiteta lastnika določenega javnega ključa. Poleg

teh podatkov pa so v digitalnem certifikatu tudi podatki o izdajatelju certifikata, datum prenehanja veljavnosti certifikata in drugi podatki.

4.1.3.3. Certifikatni uradi – overitelji javnih ključev

Danes obstajajo različne aplikacije za izdelavo javnih in zasebnih ključev, mnoge med njimi so na Internetu vsaj za testiranje na voljo tudi brezplačno. Tako si lahko vsak uporabnik sam izdela par javnega in zasebnega ključa ter ga overi z digitalnim certifikatom, vanj pa vnese povsem poljubne podatke. Če želi, se lahko izdaja tudi za povsem drugega uporabnika (tako bi se uporabnik Janko lahko izdajal za Metko).

Da bi lahko digitalnim certifikatom dejansko zaupali tako kot zaupamo potnim listom ali osebnim izkaznicam, jih morajo (podobno kot potne liste) izdajati ustrezne institucije, vredne zaupanja (Introduction to Public-Key Cryptography, 2001). Imenujemo jih »certifikatni uradi« (ang. Certificate Authority) oz. CU. CU mora pred izdajo certifikata overiti identiteto uporabnika, ki zahteva certifikat. CU so lahko neodvisne organizacije (javne ali komercialne), ki izdajajo splošno priznane certifikate, lahko pa kot CU nastopi tudi podjetje, ki certifikate izdaja svojim zaposlenim za uporabo znotraj podjetja. Da bi določena neodvisna organizacija postala splošno priznana kot CU, mora dokazati, da na ustrezen način preverja identiteto uporabnikov, ustrezno hrani njihove podatke, izdaja digitalne certifikate po ustreznih standardih (npr. X.509) ter zagotavlja javni vpogled v seznam uporabnikov, katerim je izdala digitalne certifikate. Poleg tega mora tudi podaljševati veljavnost certifikatov in preklicevati certifikate, ki niso več veljavni (na željo uporabnika, ki je npr. izgubil certifikat ali pa na lastno pobudo, ker so se npr. podatki o uporabniku spremenili).

Seznam splošno priznanih CU je na voljo na Internetu, vsebujejo pa ga tudi številne aplikacije, ki so kakorkoli povezane z Internetom (npr. spletni brskalniki). Vsaka CU, ki je na tem seznamu, svojo identiteto dokazuje s svojim javnim ključem. Če želimo, lahko seznam tudi dopolnimo[13], če pa zaradi takšnega ali drugačnega razloga izgubimo zaupanje v določen CU, ga lahko tudi izbrišemo iz seznama.

Seznam CU nam je v veliko pomoč pri preverjanju identitete lastnika določenega javnega ključa. Aplikacija (npr. spletni brskalnik) nas namreč takoj opozori, če je digitalni cerftifikat, ki vsebuje javni ključ določenega uporabnika, s katerim želimo komunicirati, izdal CU, ki ga še nimamo v seznamu overiteljev ključev. Tako bi v prejšnjem primeru, ko je Janko sam izdelal digitalni certifikat in se izdajal za Metko, lahko takoj ugotovili, da tega certifikata ni

[13] Če se odločimo zaupati kakšnemu CU, ki ga še ni na seznamu, si moramo njegov javni ključ posebej pridobiti na njegovi domači strani ali v ustreznem spletnem imeniku. Običajno moramo seznam dopolniti s slovenskimi CU, saj niso širše znani in jih zato ni na tujih seznamih splošno priznanih CU (tudi ne v slovenski verziji spletnega brskalnika Internet Explorer). Prvi slovenski CU je postal Institut Jožef Štefan, sledil pa mu je Center vlade za informatiko.

overil nobeden izmed zaupanja vrednih CU (odločitev o tem, ali takšnemu certifikatu zaupati, je seveda prepuščena vsakemu uporabniku posebej).

Vsak CU mora vzdrževati tudi seznam veljavnih certifikatov v obliki spletnega imenika certifikatov. V tem imeniku lahko vsak uporabnik Interneta dobi veljavni javni ključ lastnika certifikata, ki ga je izdal ta CU. Poleg tega mora CU vzdrževati še seznam preklicanih certifikatov (ang. *certificate revocation list* oz. *CRL*), tako da lahko vedno preverimo, ali je certifikat, s katerim se nam je predstavil določeni uporabnik Interneta, še veljaven ali ne (s tem pa tudi, ali je še veljaven njegov javni ključ).

CU vsak izdani digitalni certifikat tudi digitalno podpiše. Za podpisovanje digitalnih certifikatov pa tudi sam CU potrebuje digitalni certifikat. Tudi ta digitalni certifikat mora izdati določena CU. CU si lahko sama izda svoj digitalni certifikat, lahko pa ga pridobi od kakšne druge CU. V tem primeru govorimo o certifikatni verigi, ki jo prikazujem na sliki 5 v prilogi.

CU, ki je na vrhu certifikatne verige, si je digitalni certifikat izdal sam, hkrati pa je izdal digitalne certifikate vsem CU, ki so mu v certifikatni verigi neposredno podrejene. Ti CU so t.i. »vmesni« CU oz. VCU (ang. Subordinate Certificate Authority). Pri podpisu digitalnih certifikatov VCU navede tudi svojo mesto v certifikatni verigi. Če posamezna aplikacija (npr. spletni brskalnik) ne zaupa digitalnemu certifikatu, ki ga je izdal določen VCU (torej če tega VCU nima v seznamu CU, ki jim zaupa), preveri digitalni certifikat naslednjega CU v certifikatni verigi (vse do vrha verige)[14]. Če v tej verigi obstaja CU, ki mu aplikacija zaupa, bo zaupala tudi digitalnemu certifikatu, ki ga je izdal VCU, ki ji sicer ne zaupa. Preverjanje digitalnega certifikata prikazujem v sliki 6 v prilogi.

Če pa v celotni certifikatni verigi od začetnega VCU, ki mu aplikacija ne zaupa, do CU, ki je na vrhu certifikatne verige, ni nobenega CU, ki bi mu aplikacija zaupala, se tak digitalni certifikat zavrne in do izmenjave podatkov ne pride.

4.1.4. Zgostitveni algoritmi

Z zgostitvenimi algoritmi podatkov pravzaprav ne šifriramo, temveč le preverjamo njihovo integriteto. Rezultat kodiranja osnovnega sporočila s takšnim algoritmom je posebni *blok sporočila* oz. posebna šifra, ki je dosti krajša od osnovnega sporočila (Uporaba kriptografije – Zgostitveni algoritmi, 2002). Takšno šifro pred pošiljanjem dodamo osnovnemu sporočilu. Prejemnik nato prejeto osnovno sporočilo prav tako kodira z istim zgostitvenim algoritmom, rezultat pa preverja z blokom sporočila, ki ga je prejel poleg osnovnega sporočila. Če sta oba bloka sporočila enaka, to pomeni, da sporočilo med pošiljanjem ni bilo spremenjeno.

[14] Celotni postopek preverjanja digitalnega certifikata je povsem avtomatiziran in se izvede v nekaj sekundah, pri tem pa uporabniku Interneta ni potrebno storiti ničesar – opozorjen je le v primeru, če aplikacija ugotovi, da digitalnemu certifikatu ne more zaupati.

Zgostitveni algoritmi isto sporočilo vedno preslikajo v isti blok sporočila, iz katerega pa ni mogoče obnoviti osnovnega sporočila. Poleg tega ni moč najti dveh različnih sporočil, ki bi jih zgostitveni algoritem preslikal v isti blok sporočila. Zgostitvene algoritme lahko tako učinkovito uporabimo v boju proti eni od nevarnosti elektronskega poslovanja preko Interneta – spremembi podatkov med prenosom. Ker pa ti algoritmi niso primerni za šifriranje podatkov, s čimer bi preprečili vpogled v podatke nepooblaščenim osebam, se jih običajno uporablja le kot dodatno obliko zaščite osnovnemu šifriranju podatkov z javnimi oziroma zasebnimi ključi.

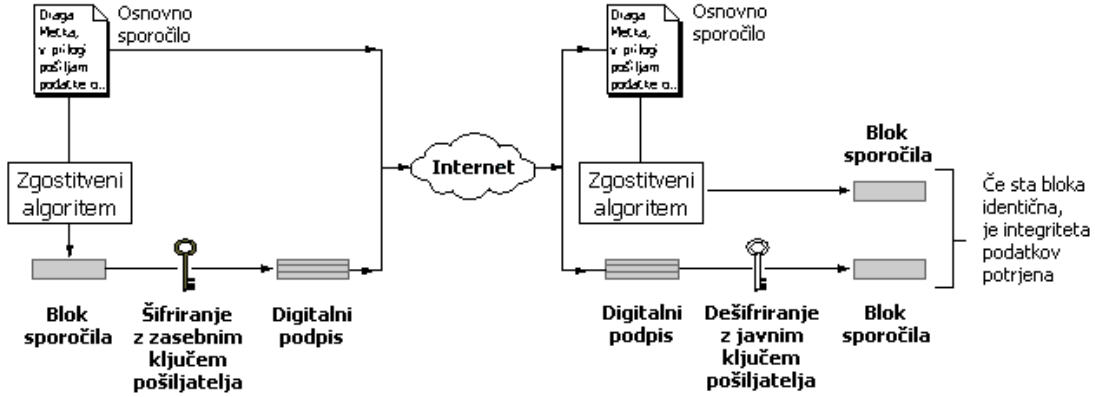
Najbolj uporabljani zgostitveni algoritmi so HMAC, MD2, MD4, MD5, SHA, SHA-1 in drugi. Do leta 1996 se je večinoma uporabljal algoritem MD5, sedaj pa prevladuje uporaba algoritma SHA-1.

4.1.5. Digitalni podpis

Digitalni podpis lahko opredelimo kot kratek šifriran podatek, ki ga dodamo šifriranemu sporočilu, zato da dokažemo integriteto podatkov in identiteto pošiljatelja.

Tehnično gledano je digitalni podpis kombinacija asimetričnega šifriranja in uporabe zgostitvenega algoritma (Danda, 2001, str. 48). Na sliki 3 prikazujem uporabo digitalnega podpisa v praksi med dvema uporabnikoma.

Slika 3: Uporaba digitalnega podpisa



Vir: Danda, 2001, str. 49.

Če želi Janko svoje sporočilo Metki tudi digitalno podpisati, mora osnovno sporočilo najprej z zgostitvenim algoritmom preslikati v blok sporočila, ki ga nato še zašifrira[15] s svojim zasebnim ključem. Rezultat šifriranja je *digitalni podpis*, ki je mnogo krajši od osnovnega

[15] Seveda se proces šifriranja (dešifriranja) ne izvaja ročno. Za to avtomatično poskrbi aplikacija, s katero Janko (Metka) pošilja (prejema) sporočila preko Interneta.

sporočila in ga aplikacija, s katero Janko pošilja sporočilo, pred pošiljanjem pripne osnovnemu sporočilu.

Seveda pa Janko s tem še ni zaščitil osnovnega sporočila: ker ne želi, da bi ga med prenosom videli tudi drugi uporabniki Interneta, ga zašifrira z Metkinim javnim ključem (če pa seveda želi, pa tudi z lastnim zasebnim ključem).

Ko Metka prejme šifrirano sporočilo, prejme tudi Jankov digitalni podpis. Najprej z Jankovim javnim ključem dešifrira digitalni podpis, s čimer dobi Jankov blok sporočila. Nato z lastnim zasebnim ključem in Jankovim javnim ključem dešifrira še šifrirano sporočilo, tako da dobi osnovno sporočilo. Ker želi preveriti integriteto sporočila (ugotoviti, ali se je sporočilo med prenosom kakorkoli spremenilo), sporočilo z istim zgostitvenim algoritmom, kot ga je uporabil tudi Janko, še sama ustvari blok sporočila, ki ga primerja z Jankovim blokom sporočila.

Če sta oba bloka sporočila enaka, je lahko prepričana, da je sporočilo prispelo nespremenjeno, v nasprotnem pa mora od Janka zahtevati, da ji sporočilo pošlje še enkrat, saj se je med prenosom poškodovalo ali pa ga je nepooblaščena oseba spremenila.

4.2. Metode šifriranja podatkov

Najširše uporabljane metode šifriranja podatkov so:

- šifriranje podatkov z uporabo programske opreme PGP,
- »infrastruktura javnih ključev« (PKI),
- SSL protokol.

4.2.1. Šifriranje podatkov z uporabo programske opreme PGP

Programska rešitev PGP (ang. Pretty Good Privacy oz. »precej dobra zaščita«) je bil eden od prvih, s katerim je bilo možno podatke pred pošiljanjem preko Interneta zašifrirati tako dobro, da jih nepooblaščene osebe ali inštitucije (niti ameriška vlada in FBI) niso mogle dešifrirati v razumnem roku (s čimer je bila dosežena dovolj visoka stopnja zaščite podatkov, da je bilo podatke mogoče varno pošiljati preko Interneta).

PGP je nastal kot odgovor na grožnje ameriške vlade, ki je v začetku devetdesetih let napovedala sprejem zakonodaje, s katero bi zelo omejila uporabo šifrirnih algoritmov. Program omogoča zelo visoko stopnjo šifriranja podatkov in danes pri tem uporablja simetrične in asimetrične algoritme, zgostitvene funkcije in vse, kar je potrebno, da lahko pošiljamo šifrirana poročila preko Interneta.

Aplikacija je imela poleg očitnih prednosti tudi določene pomanjkljivosti: sprva je temeljila na tehnologiji šifriranja s simetričnimi ključi, s čimer je seveda prevzela tudi vse pomanjkljivosti simetričnega šifriranja. Toda v začetku devetdesetih let CU še niso obstajali, zato še ni bilo možno uporabljati javnih in zasebnih ključev. Aplikacija je bila dolgo časa tudi zahtevna za uporabo, tako da ni bil primerna za vsesplošno uporabo (danes banke, borzno-posredniške hiše, trgovine in druga podjetja svoje storitve elektronskega poslovanja preko Interneta ponujajo vsem svojim komitentom, ne le visoko računalniško usposobljenim posameznikom, zato morajo biti aplikacije za uporabo teh storitev čim bolj enostavne).

Glavna pomanjkljivost PGP pri zagotavljanju varnega elektronskega poslovanja pa je bila ta, da je bil sprva namenjen predvsem šifriranju datotek in e-pošte, ne pa tudi transakcij, ki potekajo neposredno preko Interneta.

Zaradi vseh pomankljivosti simetričnega šifriranja so v ZDA začeli razvijati sistem varnega elektronskega poslovanja, poimenovan »infrastruktura javnih ključev« (PKI), ki temelji na asimetričnem šifriranju. Danes tudi PGP omogoča asimetrično šifriranje, uporabiti pa ga je mogoče tudi za šifriranje transakcij pri elektronskem poslovanju preko Interneta.

4.2.2. Infrastruktura javnih ključev (PKI)

Termin »infrastruktura javnih ključev« izhaja iz angleškega izraza »Public Key Infrastructure« (od tod tudi kratica PKI) in temelji na asimetričnem šifriranju podatkov, imenovanem tudi šifiranje z javnim ključem. Takšen način zaščite podatkov je veliko dražji od simetričnega šifriranja, saj zahteva dodatno strojno in programsko opremo, nove inštitucije, hkrati pa morajo vanj povsem zaupati tudi uporabniki, zato se je le počasi uveljavil.

Infrastruktura javnih ključev pomeni veliko več kot le skupek javnih in zasebnih ključev, digitalnih certifikatov, overiteljev javnih ključev in šifrirnih algoritmov, ki sem jih že navedel. Infrastrukturo javnih ključev lahko opredelimo kot celoto programske opreme (aplikacij), politik, delovnih in organizacijskih postopkov, splošno veljavnih načel in standardov ter zakonodaje, ki vsi skupaj opredeljujejo, kako naj deluje sistem šifriranja z javnimi ključi (Danda, 2001, str. 52). Čeprav so bili ustrezni asimetrični šifrirni algoritmi razviti že v sedemdesetih letih prejšnjega stoletja in so bile tudi vse tehnične ovire za uporabo te tehnologije pri zagotavljanju varnega elektronskega poslovanja preko Interneta sredi devetdesetih let odpravljene, pa je bila širša javnost, vključno z vladami najbolj razvitih držav in vodilnimi managerji (ki so večinoma slabo poznali tehnične podrobnosti asimetričnega šifriranja, Interneta pa niso uporabljali), do infrastrukture javnih ključev (s tem pa tudi do elektronskega poslovanja preko Interneta nasploh) precej zadržana.

Uporabniki Interneta (predvsem zaradi novega načina dokazovanja identitete posameznika) sprva niso zaupali sistemu javnih in zasebnih ključev. Ljudje se namreč običajno negativno odzovemo na vsakršne novosti, pri čemer digitalni certifikati niso bili izjema. Če podatkom v potnih listih, osebnih izkaznicah in vozniških dovoljenjih, ki jih izdajajo vladne institucije in jih je težko ponarediti, že nekaj desetletij v pretežni meri verjamemo, pa je bilo podatkom v digitalnih certifikatih sprva težko zaupati, saj so bili certifikatni uradi, ki so jih overavljali, nove in še neznane institucije. Cilj infrastrukture javnih ključev je bil izobraziti uporabnike Interneta v zvezi s sistemom javnih in zasebnih ključev ter doseči tako stopnjo zaupanja v digitalne certifikate, kot jo uživajo druge pravnoformalno določene oblike izkazovanja identitete posameznikov.

Jedro PKI predstavljajo certifikatni uradi (CU), ki sem jih že predstavil. Da bi PKI resnično postal splošno uveljavljena metoda zagotavljanja varnega elektronskega poslovanja, je bilo ključnega pomena vzpostaviti zaupanje uporabnikov v vse CU. Idealno bi seveda bilo, da bi na svetu obstajal le en CU, kateremu bi verjeli vsi uporabniki, vendar tega zaradi velike odgovornosti CU in popolne decentraliziranosti Interneta ni bilo mogoče doseči. Zato danes obstaja veliko število CU, največ pa jih je še vedno iz ZDA, kjer so najprej sprejeli ustrezno zakonodajo za reguliranje delovanja CU in uporabo digitalnih certifikatov za namene identifikacije uporabnikov Interneta. Pravna podlaga oziroma umestitev infrastrukture javnih ključev v pravni red določene države je bila zelo pomembna pri vzpostavljanju zaupanja uporabnikov v ta sistem tudi drugod po svetu.

Z vedno večjo popularnostjo Interneta so v drugi polovici devetdesetih let prejšnjega stoletja na Internet svoje poslovanje prenesla vsa večja podjetja, ki so postopoma začela sprejemati in uporabljati sistem infrastrukture javnih ključev, tako da je novi sistem dosegel kritično maso uporabnikov. Danes lahko rečemo, da je infrastruktura javnih ključev splošno uveljavljena kot glavni način zagotavljanja varnega elektronskega poslovanja preko Interneta.

4.2.3. SSL protokol

SSL protokol (ang. *Secure Socket Layer*) je eden od najbolj razširjenih šifrirnih sistemov za prenos podatkov preko Interneta. Razvilo ga je podjetje Netscape že leta 1995, danes pa ga podpirajo vsi širše uporabljani spletni brskalniki, zato se ga uporablja kot standardno rešitev tudi pri zagotavljanju varnega elektronskega bančništva. SSL protokol uporablja tri vrste šifriranja – simetrično in asimetrično šifriranje ter zgostitvene algoritme (Introduction to SSL, 2001).

Tehnično gledano je SSL varnostni nivo, ki deluje med aplikativnim nivojem procesa prenosa podatkov in TCP/IP protokolom (Introduction to SSL, 2001). Ker SSL protokol deluje pod aplikativnim nivojem procesa prenosa podatkov, lahko vse aplikacije, ki znajo uporabljati Internet, za vzpostavitev varne povezave brez težav uporabijo tudi SSL protokol.

Prednost SSL protokola je tudi ta, da ne temelji na vnaprej določenem šifrirnem algoritmu, tako da bi lahko določen algoritem v primeru, če bi zastarel ali pa bi v njem našli kakšno napako, enostavno zamenjali z drugim.

Osnova za SSL protokol so digitalni certifikati, s katerimi se subjekti, ki si želijo izmenjati podatke, predstavijo drug drugemu. Običajno gre za povezavo med spletnim strežnikom in spletnim odjemalcem. Spletni strežnik je npr. strežnik podjetja, ki svoje izdelke prodaja preko Interneta, ali pa strežnik poslovne banke, ki svojim uporabnikom omogoča tudi storitve elektronskega bančništva. Spletni odjemalec pa je lahko spletni brskalnik uporabnika Interneta ali pa kakšen drug spletni strežnik.

Za vzpostavitev SSL povezave je potreben vsaj en digitalni certifikat, saj se mora spletni strežnik vedno predstaviti spletnemu odjemalcu. Digitalni certifikat, s katerim se spletni strežnik predstavi spletnemu odjemalcu, mora podpisati (izdati) ena od CU, ki jim spletni odjemalec zaupa.

Če tudi spletni strežnik od spletnega odjemalca zahteva predstavitev, pa tudi spletni odjemalec potrebuje digitalni certifikat. Digitalni certifikat, s katerim se predstavi spletni odjemalec, mora podpisati ena od CU, ki jim zaupa spletni strežnik. V primeru, da spletni odjemalec ne zaupa spletnemu strežniku (torej ne zaupa njegovemu digitalnemu certifikatu, kar pomeni, da nima javnega ključa CU, ki je spletnemu strežniku izdala digitalni certifikat), ali pa da spletni strežnik ne zaupa spletnemu odjemalcu, do izmenjave podatkov preko SSL protokola ne bo prišlo.

SSL protokol je sestavljen iz vrste sporočil, ki si jih izmenjata strežnik in odjemalec. Vzpostavitev varne povezave, ki jo prikazujem na sliki 7 v prilogi, poteka v naslednjih korakih (Introduction to SSL, 2001):

1. Spletni odjemalec sproži zahtevek za vzpostavitev SSL povezave s spletnim strežnikom (uporabnik v spletnem brskalniku npr. odpre spletno stran na Internetu, za prikaz katere se zahteva SSL povezava). Gre za t.i. pozdravno sporočilo, v katerem spletni odjemalec strežniku pošlje tudi seznam šifrirnih algoritmov, ki jih podpira.

2. Spletni strežnik odgovori spletnemu odjemalcu. Gre prav tako za pozdravno sporočilo, v katerem se strežnik s svojim digitalnim certifikatom (v katerem je tudi njegov javni ključ) predstavi spletnemu odjemalcu, poleg tega pa mu sporoči, katere algoritme lahko odjemalec uporabi pri šifriranju podatkov.

3. Spletni odjemalec preveri veljavnost strežnikovega digitalnega certifikata. Poleg drugih podatkov preveri tudi, ali je ime strežnika, navedeno v certifikatu, enako dejanskemu

imenu strežnika, kot je to dejansko navedeno na Internetu[16]. Če je potrebno (če to zahteva spletni strežnik), se tudi spletni odjemalec z digitalnim certifikatom predstavi spletnemu strežniku.

4. Spletni odjemalec izdela unikatni šifrirni ključ za kasnejše simetrično šifriranje podatkov[17] ter ga zašifrira s strežnikovim javnim ključem in ga pošlje strežniku.

5. Spletni strežnik in spletni odjemalec si izmenjata še zadnji pozdravni sporočili: ti med drugim vsebujeta blok dotedanje komunikacije (narejen z zgostitvenimi algoritmi) med strežnikom in odjemalcem. S primerjavo lastnega in prejetega bloka odjemalec preveri integriteto poslanih podatkov. Če se oba bloka ujemata, se nepooblaščene osebe niso vmešale v prenos podatkov, tako da je odjemalec lahko potrdi, da je vzpostavil varno povezavo s strežnikom.

Po vzpostavitvi varne SSL povezave si spletni strežnik in odjemalec lahko začneta izmenjevati podatke. Podatke simetrično šifrirata z dogovorjenim algoritmom, pri čemer uporabita unikatni šifrirni ključ, ki je bil izdelan prav za to povezavo.

Glede na izbiro šifrirnega algoritma ter lastnosti spletnega strežnika in odjemalca so za vzpostavitev varne SSL povezave lahko potrebni še dodatni koraki (Danda, 2001, str. 58). Včasih (pri določenih šifrirnih algoritmih) se npr. unikatni šifrirni ključ uporabi za izdelavo dodatnih unikatnih šifrirnih ključev, s katerimi se potem dejansko šifrirajo podatki, ki se prenašajo preko Interneta. V tem primeru odjemalec strežniku najprej pošlje »predhodno« šifro (ang. premaster secret), na podlagi katere tako odjemalec kot strežnik najprej na podlagi istih algoritmov izdelata »glavno« šifro (ang. master secret), na podlagi te pa šele unikatni šifrirni ključ.

4.3. Načini dokazovanja identitete uporabnikov

Poleg metod za šifriranje podatkov se za večjo varnost elektronskega bančništva uporabljajo tudi dodatne metode dokazovanja identitete. Kljub splošni uveljavitvi infrastrukture javnih ključev le ena stopnja dokazovanja identitete ne zadošča za res varno elektronsko

[16] Ta korak je potreben za preprečitev nevarnosti prevzema identitete. V tem primeru bi lahko nepooblaščena oseba izvedla t.i. *napad moža v sredini* (ang. man-in-the-middle attack) tako da bi se s posebnim programom vmešala v komunikacijo med spletnim strežnikom in odjemalcem in se odjemalcu predstavila kot strežnik, strežniku pa kot odjemalec. Nato bi prestregla šifrirni ključ, s čimer bi imela neoviran dostop do podatkov, ki bi si jih izmenjevala strežnik in odjemalec. Zato mora odjemalec posebej preveriti dejansko Internetno ime strežnika (tega imena nepooblaščena oseba ne more spremeniti), ter ga primerjati z imenom, navedenim v digitalnem certifikatu, s katerim se mu je strežnik predstavil. Če se imeni ne ujemata, odjemalec prekine z vzpostavljanjem varne SSL povezave.

[17] Šifrirni ključ vedno izdela spletni odjemalec, saj v primeru, da bi ga izdelal spletni strežnik, ne bi imeli zagotovila, da je šifrirni ključ vedno unikaten – spletni strežnik bi lahko isti šifrirni ključ uporabljal tudi pri komunikaciji z drugimi spletnimi odjemalci. V tem primeru pa s simetričnim šifriranjem ne bi bilo več možno ustrezno zaščititi podatkov, saj šifrirni ključ ne bi bil znan le pošiljatelju in prejemniku teh podatkov.

poslovanje. Ljudje namreč nismo nezmotljivi, zato lahko naš digitalni certifikat dobijo v roke tudi nepooblaščene osebe (lahko izgubimo disketo z rezervno kopijo certifikata; certifikat lahko iz domačega računalnika prenesemo na službenega, do katerega imajo dostop tudi drugi zaposleni; domači računalnik dovolimo uporabljati tudi otrokom in prijateljem itd). Zato je priporočljivo, da ponudniki storitev elektronskega poslovanja poleg digitalnega certifikata od uporabnikov zahtevajo dodatno še dokazovanje identitete (podobno kot bankomat od nas zahteva tako predložitev bančne kartice kot osebnega gesla). Tudi uporabniki bi takšne zahteve morali pozdraviti, saj koristijo predvsem njim, in z nezaupanjem sprejemati tiste spletne ponudnike raznovrstnih storitev, ki od njih tega ne bi zahtevali, saj bi z upravičenostjo lahko dvomili v varnost takšne izmenjave podatkov.

Nekatere izmed metod ugotavljanja identitete izhajajo še iz obdobja, ko infrastruktura javnih ključev ni bila splošno uveljavljena, druge pa se šele uveljavljajo z razvojem novih tehnologij za biometrično preverjanje identitete uporabnika.

Med načine dokazovanja identitete (poleg infrastrukture javnih ključev) uvrščamo predvsem:

- vnos uporabniškega imena in/ali (enkratnega časovnega) gesla;
- podpis z digitalnim peresom;
- biometrične metode.

Vnos uporabniškega imena in/ali gesla bi bila v kombinaciji s SSL protokolom povsem sprejemljiva v primeru, če bi jo izvajali le na ravni računalnikov oz. računalniških aplikacij. Vendar pa uporabniška imena in gesla uporabljamo ljudje, ki jih velikokrat pozabimo, shranimo na javno dostopno mesto (na trdi disk računalnika, disketo, list papirja, na nalepko, ki jo pustimo kar ob zaslona računalnika), jih zaupamo sorodniku ali prijatelju ali pa si izberemo takšno geslo, ki ga lahko brez težav ugotovijo tudi drugi. V splošnem velja, da je navedba uporabniškega imena in/ali gesla v kombinaciji z uporabo infrastrukture javnih ključev zadosten, ne pa najboljši dokaz identitete uporabnika.

Zato je bilo potrebno razviti bolj kompleksne metode dokazovanja identifikacije uporabnikov. Ena od njih je uporaba enkratnih časovnih gesel - uporabnik prejme unikatni kalkulator osebnih gesel ter osebno šifro za uporabo kalkulatorja. Pri vsaki prijavi v sistem najprej vnese osebno šifro v kalkulator osebnih gesel, ta pa mu izračuna unikatno geslo, ki velja zanj v tistem trenutku. Tristopenjski način dokazovanja identitete uporabnikov z digitalnim certifikatom, uporabniškim imenom (ki bi bilo znano le vsakemu posameznemu uporabniku posebej) in enkratnim časovnim geslom je povsem zadovoljiva metoda identifikacije uporabnika za potrebe elektronskega bančništva.

Ob dosledni uporabi infrastrukture javnih ključev in takšni dodatni zahtevi dokazovanja identitete uporabnikov bi bila nevarnost vmešavanja v prenos podatkov s strani nepooblaščenih oseb skoraj izključena (oziroma bi bila nekajkrat manjša kot je nevarnost

zlorabe pri običajnem poslovanju, npr. pri vsakodnevni uporabi plačilnih in kreditnih kartic). Žal pa v Sloveniji še nobena poslovna banka ne zahteva tako kompleksnega dokazovanja identitete svojih uporabnikov.

Poleg uporabniških imen in gesel so v svetu razvili še druge načine dokazovanja identitete uporabnikov. Eden od teh je podpis z digitalnim peresom po sistemu PenOp (Toplišek, 1998, str. 35). Sistem PenOp ima dve osnovni sestavini: sistem za zajemanje podpisa (ki je sestavljen iz strojne in programske opreme) in sistem za preverjanje podpisa. Sistem bi prav tako kot prej omenjene metode dovolj zadovoljivo rešil problem identifikacije uporabnika, poleg tega pa bi se digitalizirani elektronski podpis lahko dodal samemu sporočilu in tako zagotovil tudi integriteto podatkov (s čimer bi odpravil tudi problem spreminjanja podatkov med prenosom), vendar med uporabniki Interneta zaradi prevelikih stroškov strojne opreme, potrebne za njegovo uporabo, ni doživel večjega uspeha.

V prihodnosti lahko pričakujemo razvoj različnih biometričnih metod dokazovanja identitete uporabnikov. Ameriška davčna služba je v devetdesetih letih prejšnjega stoletja preizkušala elektronsko sprejemanje davčnih napovedi, pri čemer je kot metodo ugotavljanja identitete pošiljatelja uporabila njegovo glasovno sporočilo (Toplišek, 1998, str. 32). Danes se kot biometrični dokaz identitete uporabnika najpogosteje omenja t.i. »test oči« oziroma dela očesa (šarenice), ki prav tako enolično določa vsakega človeka in ga je nemogoče ponarediti (ali, kot je primer npr. pri geslih, na takšen ali drugačen način izvedeti od drugega uporabnika).

Za večjo razširjenost in uporabnost takšnih metod preverjanja identitete uporabnikov pa bo najprej potrebno razviti cenovno sprejemljivo strojno opremo, ki za sedaj še ni na voljo. Trenutno se ta način preverjanja identifikacije uporablja le v resničnem svetu, npr. pri vstopu v določene objekte, kjer potrebujemo le nekaj tovrstnih naprav za preverjanje identitete. Ker pa uporabniki Interneta storitve elektronskega bančništva opravljajo preko svojih računalnikov individualno (ne pa na nekem določenem skupnem mestu), bi za zagotovitev varnega elektronskega bančništva z uporabo biometričnih metod dokazovanja identitete vsak uporabnik potreboval svojo napravo za preverjanje identitete, kar pa je zaradi že omenjenih previsokih cen tovrstnih naprav trenutno še neizvedljivo.

4.4. Kriteriji za izbiro ponudnika elektronskega bančništva

Elektronsko bančništvo v Sloveniji danes ponujajo praktično vse poslovne banke, pri čemer so za varnost takšnega poslovanja poskrbele na različne načine, ki sicer večinoma temeljijo na infrastrukturi javnih ključev, vendar pa so le redke banke izkoristile vse možnosti, ki jih ta tehnologija ponuja.

V pogojih konkurence pri opravljanju storitev plačilnega prometa bodo podjetja pri izbiri poslovne banke (ali bank), pri kateri bodo opravljale te storitve, verjetno upoštevala predvsem ekonomske kriterije, kot so strošek posamezne transakcije, ponudbo povezanih bančnih storitev, fleksibilnost, ugled banke itd.

Zaradi želje po racionalizaciji poslovanja bodo podjetja želela uporabljati tudi rešitve elektronskega bančništva. Zato bi morala pri izbiri poslovne banke preveriti, katere tržne poti jim banka ponuja – spletnega odjemalca, programskega odjemalca itd., kakšno funkcionalnost vsebuje vsaka od teh rešitev ter kako je možno posamezno bančno rešitev povezati z informacijskim sistemom podjetja.

Poleg navedenih pa bi podjetja pri izbiri posrednika za opravljanje storitev plačilnega prometa morala preveriti vsaj naslednje varnostne kriterije:

- ali banka podjetju izda digitalni certifikat;
- kakšna dodatna identifikacija se zahteva poleg predložitve digitalnega certifikata;
- kakšne načine shranitve digitalnega certifikata ponuja banka.

Kljub temu, da večina bank danes za varnost elektronskega bančništva uporablja infrastrukturo javnih ključev, pa nekatere banke uporabnikom kljub temu ne izdajajo digitalnih certifikatov. Čeprav je tudi takšna rešitev tehnično še sprejemljiva, saj je šifriranje podatkov s SSL protokolom možno izvesti tudi brez odjemalčevega certifikata, pa je vseeno priporočljivo, da podjetja zahtevajo od banke lastni digitalni certifikat. Le-ta je namreč posebni digitalni dokument, ki ga je izredno težko ponarediti, hkrati pa omogoča dodatne varnostne funkcije, kot je npr. digitalni podpis.

Kot sem že omenil v prejšnji točki, je zelo pomembna tudi dodatna identifikacija uporabnikov. Nekatere banke pri tem zahtevajo le osebno geslo, spet druge uporabljajo sistem uporabniških imen in gesel, le redke pa ponujajo tudi sistem enkratnih časovnih gesel. Najvarnejša rešitev je zahteva po predložitvi digitalnega certifikata, kombinirana z zahtevo po vnosu uporabniškega imena in enkratnega časovnega gesla, vendar pa take zaščite ne ponuja še nobena slovenska banka. Prav tako se še ne uporabljajo drugi načini preverjanja identitete uporabnikov (npr. različne biometrične metode).

Posebno pozornost pa morajo podjetja posvetiti shranjevanju digitalnih certifikatov. Osnovna rešitev je shranjevanje certifikatov na trdi disk računalnika, kar je obenem tudi najslabša možnost, saj je certifikat, ki na trdem disku obstaja v obliki datoteke, možno enostavno prenesti na disketo ali drug računalnik. Podjetja bi zato od banke morala zahtevati posebno »pametno« kartico, na kateri je digitalni certifikat shranjen mnogo bolj varno. Kartica za uporabo zahteva posebno napravo (čitalec pametnih kartic), pred vsako uporabo pa mora lastnik kartice vnesti še posebno osebno geslo, da aplikacija pridobi dostop do digitalnega certifikata. Prenašanje certifikata iz pametne kartice (na način, kot je to npr.

možno pri hranjenju certifikata na trdem disku) ali njegovo razmnoževanje pa je povsem onemogočeno.

V zadnjem času nekatere banke ponujajo tudi novo rešitev – t.i. »pametni« ključ, ki za uporabo ne potrebuje posebnega čitalca, temveč ga je možno priklopiti na USB vrata računalnika, zato je cenovno ugodnejša in bolj fleksibilna rešitev od pametne kartice. Prav tako kot pametna kartica tudi pametni ključ ne omogoča direktnega dostopa do digitalnega certifikata, tako da ni možno njegovo prenašanje (in s tem npr. kraja), omogoča pa lažjo uporabo na različnih računalnikih, saj je potrebno s seboj nositi le majhen ključ, ne pa mnogo večje kartice in čitalca.

Šele na podlagi vseh teh informacij o ponudbi bančnih storitev lahko podjetja oblikujejo objektivno oceno, ali je določeni poslovni banki smiselno zaupati opravljanje storitev plačilnega prometa. Odločanje le na podlagi ekonomskih ali le na podlagi varnostnih kriterijev namreč ni ustrezno in lahko vodi v napačne odločitve, ki ne bodo pripomogle k racionalnosti poslovanja.

Sklep

Reforma plačilnih sistemov v Republiki Sloveniji je bila nujna zaradi prehoda iz socialističnega v tržno gospodarstvo, ki zahteva konkurenco tudi na področju opravljanja plačilnega prometa in ne pozna družbene lastnine, nad katero bi se moral izvajati nadzor. V Sloveniji smo se reforme lotili počasi, zato je trajala skoraj desetletje, vendar se z junijem letošnjega leta projekt vendarle zaključuje.

Reforma za podjetja prinaša več kot le prenos plačilnega prometa iz Agencije za plačilni promet v banke, saj je razvoj informacijskih in telekomunikacijskih tehnologij v zadnjem desetletju bankam omogočil ponudbo novih tržnih poti, ki temeljijo na elektronskem bančništvu, pri čemer se za prenos podatkov uporablja nov medij Internet.

Internet pa v svoji zasnovi ni bil zamišljen kot medij za prenos zasebnih podatkov, zato je bilo potrebno vzpostaviti mehanizme varnega prenosa podatkov ter med uporabniki doseči dovolj visoko stopnjo zaupanja v nove tehnologije. To je bilo možno šele z uporabo SSL protokola v kombinaciji s tehnologijo infrastrukture javnih ključev, ki so ju razvili sredi devetdesetih let prejšnjega stoletja.

Šifriranje podatkov z uporabo SSL protokola nepooblaščenim osebam onemogoči vpogled v podatke, ki se prenašajo preko Interneta, za preprečitev drugih možnosti vmešavanja v prenos podatkov pa uporabimo možnosti infrastrukture javnih ključev. Z digitalnim

podpisom preprečimo nevarnost spremembe podatkov med prenosom, z obvezno uporabo digitalnih certifikatov tako pošiljatelja kot prejemnika podatkov pa se zagotovi ustrezna identifikacija vseh sodelujočih pri prenosu podatkov. Tehnologija infrastrukture javnih ključev temelji na sistemu javnih in zasebnih ključev in zaupanju v izdane digitalne certifikate, ki jih izdajajo certifikatni uradi. Zaradi svoje kompleksnosti se je tehnologija le počasi uveljavila, zato so se v preteklosti bolj uporabljali drugi, bolj preprosti načini zagotavljanja varnosti, danes pa SSL protokol v kombinaciji z infrastrukturo javnih ključev uporabljajo praktično vsi ponudniki varnega elektronskega poslovanja.

Za večjo varnost pri elektronskem bančništvu se poleg SSL protokola in infrastrukture javnih ključev uporabljajo tudi različni sistemi za dodatno preverjanje identitete uporabnika. Poleg predložitve ustreznega digitalnega certifikata se od uporabnika zahteva tudi vnos uporabniškega imena in/ali osebnega gesla, s čimer se rešuje problem prevzemanja identitete s strani nepooblaščenih oseb. Do zlorab lahko pride le v primeru nepazljivosti uporabnikov, tako da ob takšnem načinu preverjanja identitete uporabnikov elektronsko bančništvo ne prinaša večjega tveganja kot siceršnje poslovanje, kjer mora uporabnik pri uporabi bankomata poleg predložitve bančne kartice (ki jo skoraj nemogoče ponarediti, lahko pa jo izgubimo, tako da je po tem vidiku povsem primerljiva z digitalnim certifikatom) prav tako vnesti osebno šifro. Le od vsakega posameznika je odvisno, kako bo hranil svoj digitalni certifikat in osebno geslo, tako kot je le od vsakega posameznega uporabnika elektronskega poslovanja odvisno, kako bo hranil svojo bančno kartico in osebno šifro.

Podjetja pa morajo biti pri izbiri ponudnika za opravljanje plačilnega prometa vseeno zelo previdna. Po preučitvi ekonomskih kriterijev, med katere spadajo strošek posamezne transakcije, ponudba drugih bančnih storitev, fleksibilnost banke in njen ugled, je potrebno podrobno preveriti tudi ponudbo banke na področju elektronskega bančništva. Podjetje mora najprej oceniti možnost integracije rešitve elektronskega bančništva, ki jo ponuja banka, z informacijskim sistemom podjetja, nato pa mora preveriti metode zaščite podatkov, ki jih banka uporablja pri njihovem prenosu preko Interneta. Zelo pomembna je tudi zaščita digitalnega certifikata, ki jo ponuja banka. Podjetja morajo namreč skrbno hraniti svoj digitalni certifikat z zasebnim ključem, saj ga potrebujejo za identifikacijo, zato ga ne smejo pridobiti nepooblaščene osebe. Najprimernejše mesto za hranjenje digitalnega certifikata je pametna kartica, s katere je certifikat nemogoče fizično prenesti, saj je do njega možen dostop samo prek ustrezne aplikacije. V zadnjem času pametno kartico vse bolj nadomešča pametni ključ, ki je manjši in enostavnejši za uporabo.

Glede na številne tržne poti, ki jih ponujajo poslovne banke, imajo danes podjetja veliko večjo izbiro različnih načinov opravljanja plačilnega prometa, kot pa so jih imela pred reformo plačilnih sistemov, s konkurenco na trgu in uvedbo novih tržnih poti pa so se znižali tudi stroški transakcij. Zato lahko proces prenosa plačilnega prometa v okvir poslovnih bank kljub velikim zamudam pri izvedbi projekta ocenimo kot zelo uspešnega.

Literatura

1. Bauer Friedrich L.: Decrypted Secrets. Berlin: Springer, 1997. 447 str.

2. Danda Matthew: Protect Yourself Online. Redmond: Microsoft Press, 2001. 368 str.

3. Grujakovič Nataša: Plačilni sistemi v Sloveniji in drugih evropskih državah. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2002. 48 str.

4. Logar Romana: Plačilni sistemi. Ljubljana: Slovenski inštitut za revizijo, 1998. 412 str.

5. Posel Barbara: Reforma plačilnega sistema v Sloveniji. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 1997. 41 str.

6. Strokovno posvetovanje Prenos plačilnega prometa na banke in naloge v podjetjih. Ljubljana: Društvo ekonomistov Ljubljana, 2000, 58 str.

7. Prijanovič Boštjan: Reforma plačilnega prometa. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 1997. 46 str.

8. Pržulj Nataša: Prenos plačilnega prometa iz APP v banke in njegov vpliv na poslovanje podjetij. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2001. 50 str.

9. Sistemi bančništva na daljavo. [URL:http://www.zaslon.si/bancnistvo/trzne_poti.htm], 8.5.2000.

10. Strategija migracije plačilnega prometa v projektu reforme, 1996).

11. Summers Bruce J.: The Payment System: design, management and supervision. Washington D.C.: International Monetary Fund, 1994. 214 str.

12. Šušteršič Darja: Smiselnost oglaševanja čistilnih sredstev na Internetu v Sloveniji. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2001. 45 str.

13. Toplišek Janez: Elektronsko poslovanje.Ljubljana: Atlantis, 1998. 336 str.

Viri

1. Computer Industry Almanac. [URL: http://www.c-i-a.com/200010iuc.htm], 10.8.2001.

2. European Commission: Directorate-General XIII, Ensuring Security and Trust in Electronic Communication. [http://www.ispo.cec.be/eif/policy/97503toc.html], 1.2.1997.

3. Informacijska tehnologija. [URL: http://lsd.uni-mb.si/slo/studenti/epf/Predanvanja03.pdf], 10.4.2002.

4. International Survey of E-Commerce. [URL:http://www.witsa.org/ papers/EcomSurv.pdf], 15.10.2000.

5. Introduction to Public-Key Cryptography. [http://docs.iplanet.com/docs/manuals/security/pkin/contents.htm], 11.11.2001.

6. Introduction to SSL. [http://docs.iplanet.com/docs/manuals/security/sslin/contents.htm], 11.11.2001.

7. Kisli zmagovalci plačilne reforme. [URL:http://www.finance-on.net/show.php?id=21645], 8.5.2002.

8. Potrebe po spremembi slovenskega plačilnega sistema. Banka Slovenije, 1994.

9. Reforma plačilnega prometa se bliža koncu. [URL:http://www.finance-on.net/show.php?id=21640], 8.5.2002.

10. S programom pospeševanja bo odprtih več tisoč računov. [http://www.finance-on.net/show.php?id=24212], 20.5.2002

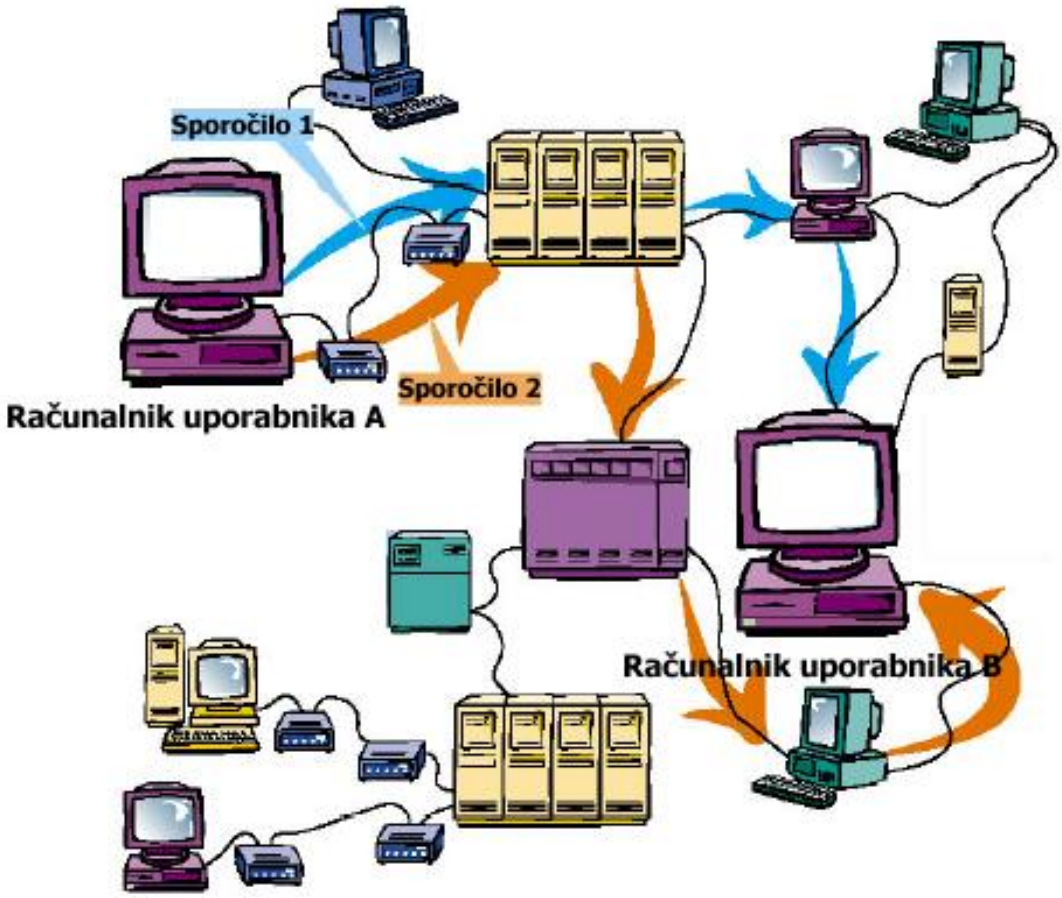
11. Uporaba kriptografije – Simetrični algoritmi. [http://www.gov.si/tecaj/kripto/kr-sim.htm], 15.4. 2002.

12. Uporaba kriptografije – Zgostitveni algoritmi. [http://www.gov.si/tecaj/kripto/kr-zgo.htm], 15.4. 2002.

13. Uporaba kriptografije - XOR [URL:http://www.gov.si/tecaj/kripto/xor.htm], 15.4.2002.

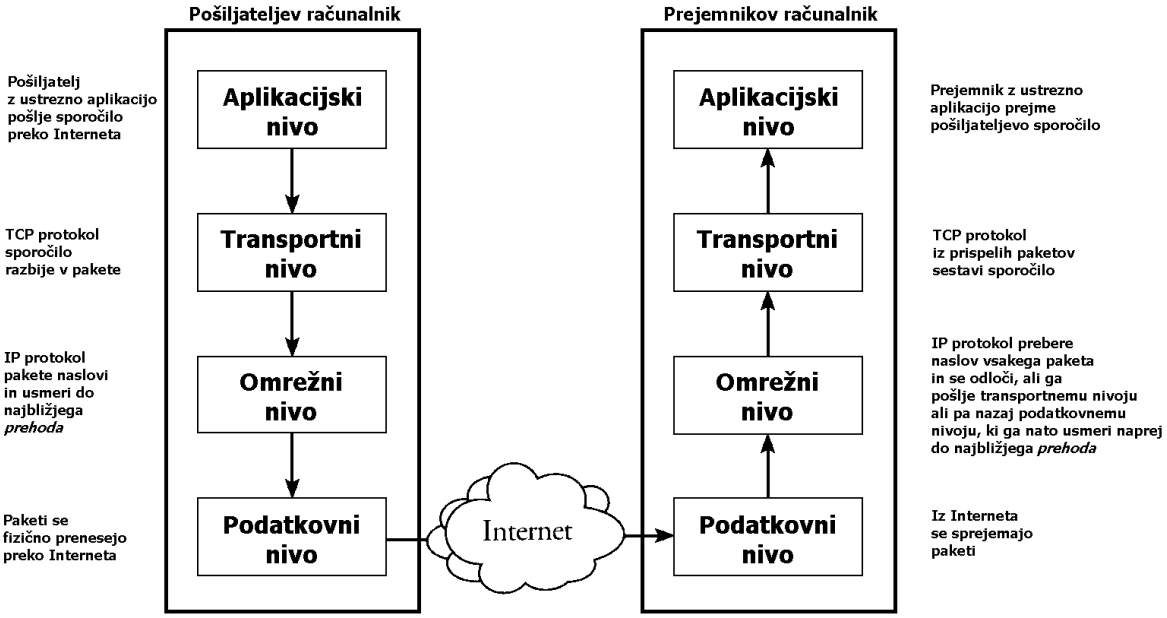
PRILOGE

Slika 1: Prenos podatkov preko Interneta



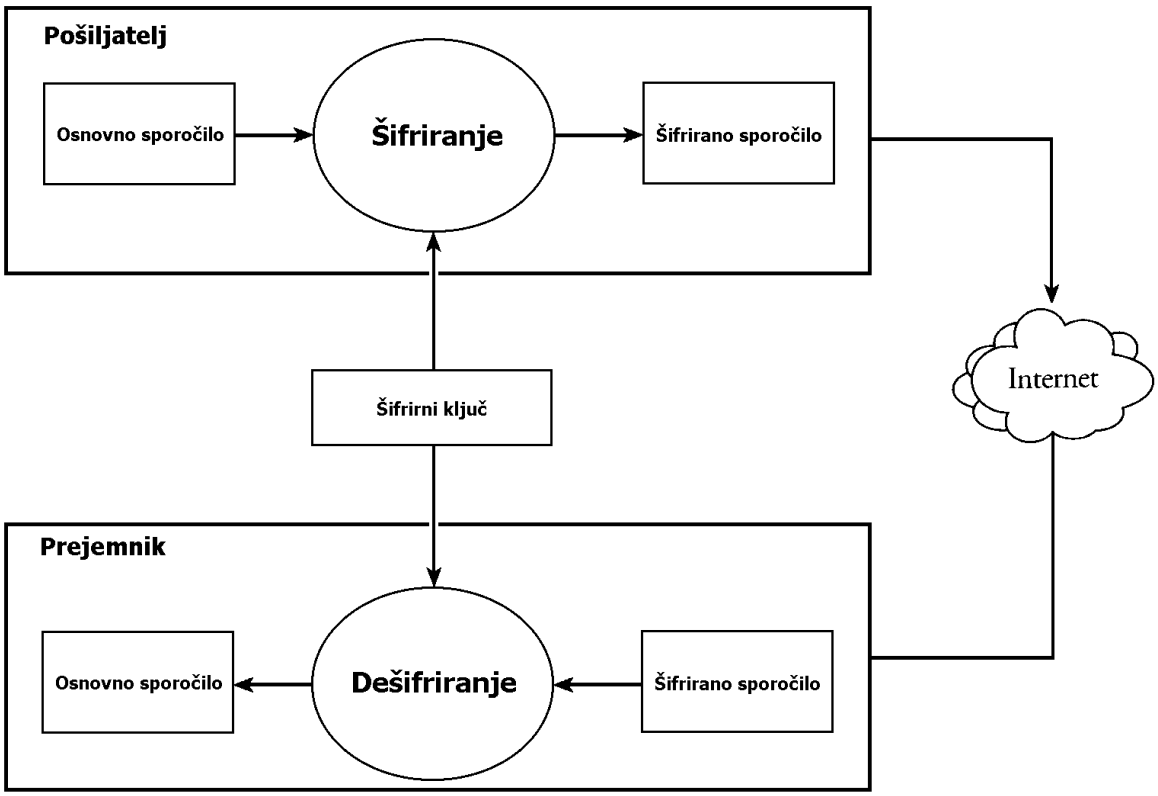
Vir: Informacijska tehnologija, 2002.

Slika 2: Prenos podatkov preko Interneta



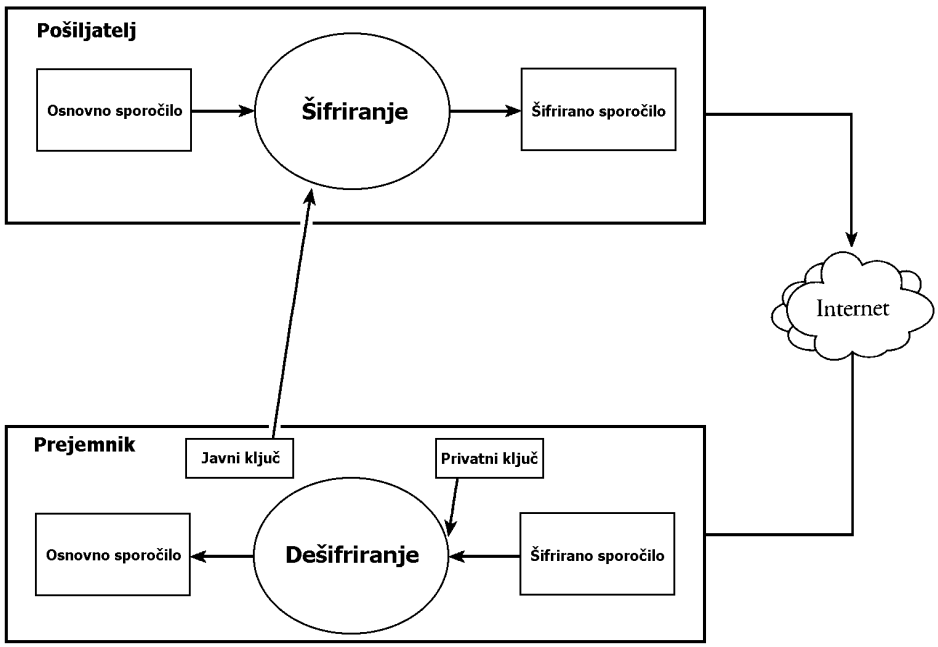
Vir: Danda, 2001, str. 21.

Slika 3: Simetrično šifriranje



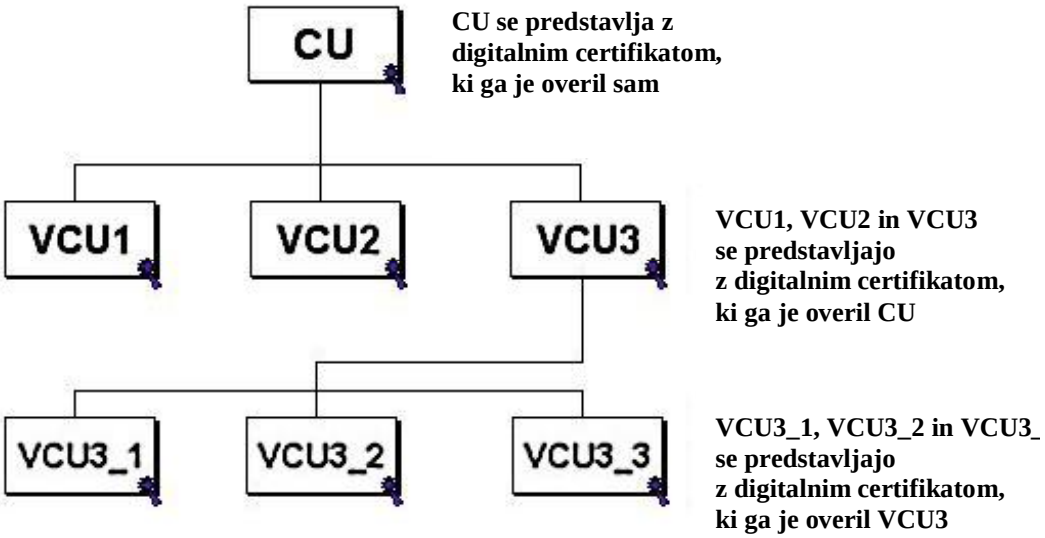
Vir: Danda, 2001, str. 43.

Slika 4: Asimetrično šifriranje



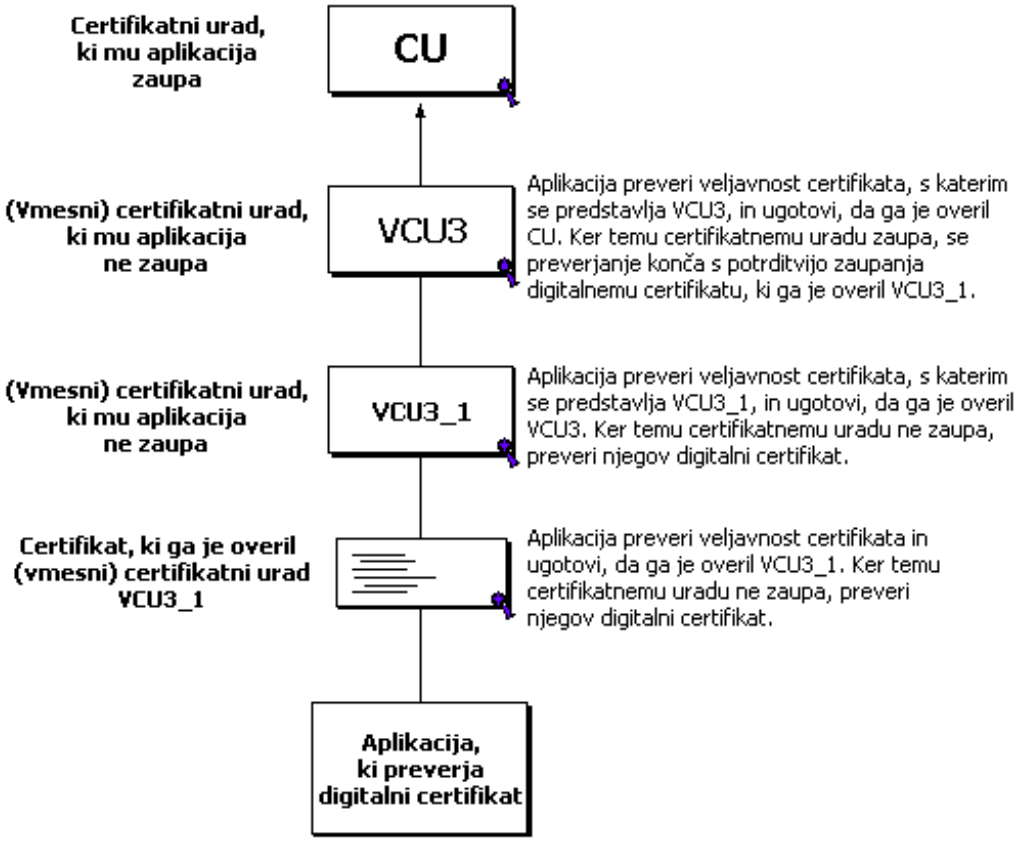
Vir: Danda, 2001, str. 47.

Slika 5: Certifikatna veriga



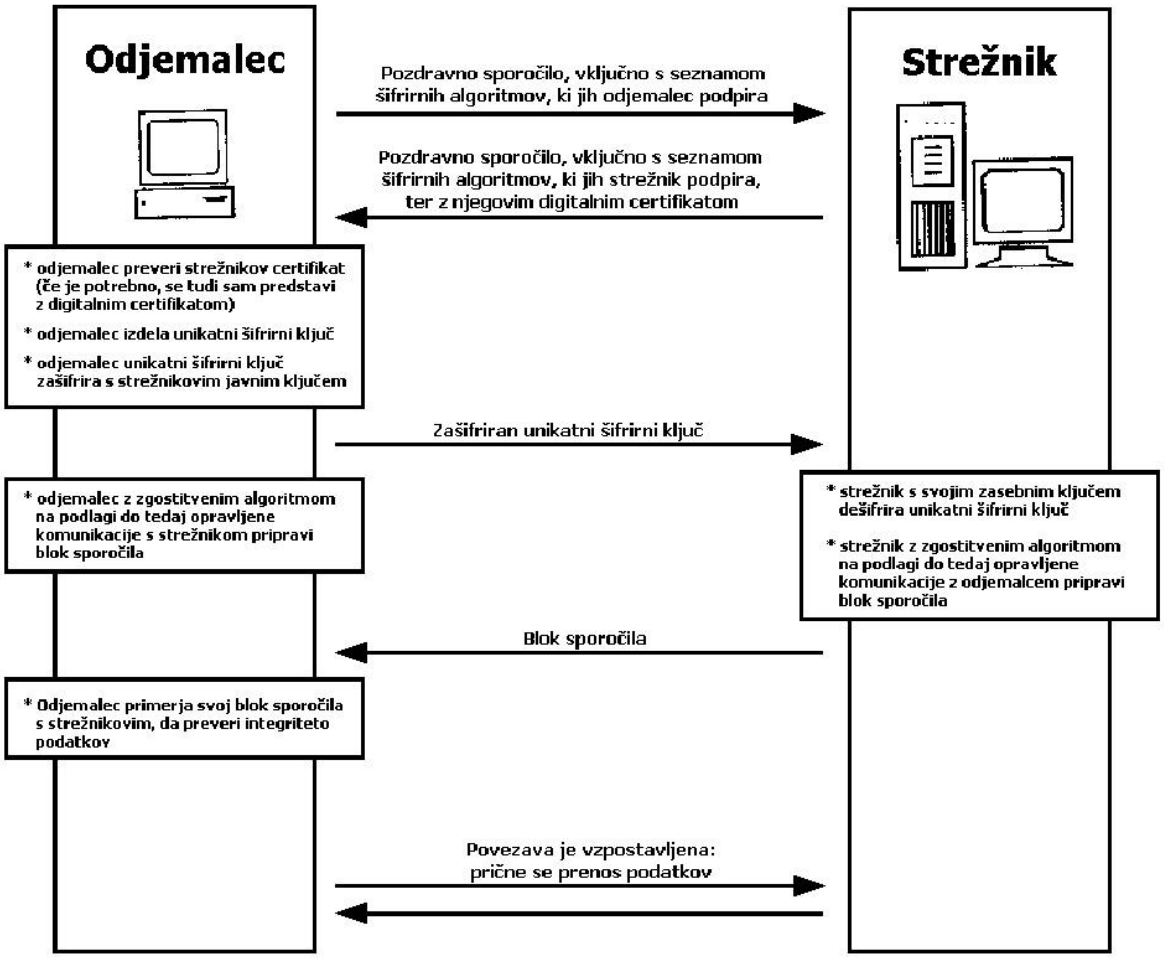
Vir: Introduction to Public-Key Cryptography, 2001.

Slika 6: Preverjanje digitalnega certifikata



Vir: Introduction to Public-Key Cryptography, 2001.

Slika 7: Vzpostavitev varne povezave s SSL protokolom



Vir: Danda, 2001, str. 57.

Slika 8: Obvestilo brskalnika, da pričenja vzpostavljati varno povezavo s strežnikom

Slika 9: Opozorilo brskalnika, da ne zaupa certifikatu, s katerim se je predstavil strežnik (overitelja digitalnega certifikata strežnika ni v brskalnikovem seznamu)

Slika 10: Opozorilo brskalnika v primeru potencialnega napada »moža v sredini« (internetno ime strežnika ni enako imenu, zapisanem v certifikatu)