UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

PRIMERJALNA ANALIZA VARNOSTI UPORABE SODOBNIH PLAČILNIH INSTRUMENTOV

Ljubljana, marec 2002 VLADANKA LOVIĆ

IZJAVA

Študentka Vladanka Lović izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom mag. Aleksandre Gregorič, in dovolim objavo diplomskega dela na fakultetni domači strani.

V Ljubljani, dne _____ Podpis:

KAZALO

1. UVOD

Bankomati, plačilne kartice, telefonska banka, elektronsko bančništvo preko interneta in v zadnjem času še mobilno bančništvo tudi v Sloveniji korenito spreminjajo tradicionalni način poslovanja z bankami. Gre za vedno nove in nove načine poravnavanja obveznosti in poslovanja z bankami, ki so poznane pod skupnim imenom elektronsko bančništvo[1].

V Sloveniji za poravnavo obveznosti vse bolj uporabljamo sodobne plačilne instrumente. V velikem porastu je predvsem uporaba tako imenovanega plastičnega denarja - plačilnih kartic in bančnih avtomatov, medtem ko se uporaba čeka kot plačilnega instrumenta postopno zmanjšuje. Počasi se povečuje tudi število uporabnikov telefonskega bančništva. V času, ko je računalnik prisoten že skoraj v vsaki slovenski družini ter se število priklopov na internet povečuje in ko narašča število uporabnikov mobilnih telefonov, lahko pričakujemo velik interes tudi za elektronsko in mobilno bančništvo. Mobilno bančništvo je bančna storitev prihodnosti, saj bo uporabnikom omogočeno opravljanje bančnih storitev resnično od kjerkoli in kadarkoli.

Glede na to, da uporaba sodobnih plačilnih instrumentov narašča, se postavlja vprašanje, kako varno je poslovanje z njimi. Za zagotovitev varnega poslovanja je pomembno, da imajo dostop do podatkov le pooblaščene osebe in da s temi podatki upravljajo le v okviru svojih pooblastil. Vsak prenos podatkov ali dostop do sistema z dragocenimi podatki je nevaren, saj razkritje ali uničenje takih podatkov lahko povzroči neprecenljivo škodo. Zato sem se odločila, da v svojem diplomskem delu obravnavam najsodobnejše plačilne instrumente z vidika njihove varnosti.

Namen diplomskega dela je raziskati, kateri so sodobni plačilni instrumenti, kako je z njihovo uporabnostjo v Sloveniji, kako je poskrbljeno za varnost poslovanja z njimi, hkrati pa sem poskusila odkriti, kakšne so zlorabe na tem področju.

Cilj diplomskega dela je pridobiti celovito informacijo o varnosti posameznih plačilnih instrumentov s poudarkom na varnosti poslovanja elektronskega bančništva. Tako sem v diplomskem delu po posameznih poglavjih predstavila poslovanje s plačilnimi karticami, elektronsko, mobilno bančništvo, poslovanje preko bankomatov, telefonsko bančništvo in

[1] V nadaljevanju bom z izrazom elektronsko bančništvo označevala elektronsko bančništvo preko interneta.

poslovanje s čekom. Predstavitev dopolnjujem z primerjalno analizo varnosti uporabe navedenih sodobnih plačilnih instrumentov. V zadnjem poglavju sem predstavila še zlorabe na področju plačilnih kartic, interneta in elektronskega bančništva.

2. PLAČILNE KARTICE

Plačilna kartica se je "rodila" zaradi pozabljivosti. Ameriški poslovnež Frank McNamara je po odlični večerji v eni od ameriških restavracij zgroženo ugotovil, da je pozabil denarnico. Ko mu je natakar prinesel račun, se je znašel v nerodni situaciji, zato se je "izmazal" z dogovorom o odlogu plačila. Ideja o kartici kot osnovnemu sredstvu za brezgotovinsko poslovanje je bila torej rojena. Tako so prvo kartico v ZDA izdali 20. februarja 1950 (Diners). American Express se je pojavila leta 1959, nekaj let kasneje pa še MasterCard in Visa (Klapš, 1995, str. 22).

2. 1. Plačilne kartice v Sloveniji

Plačilna kartica se uporablja pri opravljanju drobnoprodajnih plačil. Opravlja dve funkciji, in sicer identificira prinosnika in izdajatelja kartice ter v očeh prodajalca vzpostavi zahtevano kredibilnost kupca.

Tabela 1: Uporaba plačilnih kartic glede na število plačil v Sloveniji od leta 1996 do 2000

	1996	1997	1998	1999	2000
kreditne	24.259.714	30.998.115	38.239.666	44.193.580	51.933.000
• domače	18.542.593	21.980.757	25.992.672	28.395.532	31.830.000
• licenčne	5.717.121	9.017.358	12.244.994	15.798.048	20.103.000
• bančne	18.418.818	23.114.001	28.146.605	33.049.969	38.426.000
• podjetniške	5.840.896	7.884.114	10.091.061	11.143.611	13.506.000
• osebne	21.315.005	27.105.829	33.231.308	38.703.697	44.209.000
• poslovne	2.944.709	3.892.286	5.006.358	5.489.833	7.724.000
debetne		44.536	1.216.309	5.265.989	13.933.000
tuje	1.212.108	1.755.296	2.277.998	2.924.634	3.745.000

Vir: Šteblaj, 2000, str. 45-55 in http://www.bsi.si.

Tabela 2: Število izdanih plačilnih kartic v Sloveniji od leta 1996 do leta 2000

	1996	1997	1998	1999	2000
kreditne	468.912	594.717	593.863	647.816	742.071
• domače	309.259	382.150	350.567	374.929	421.405
• licenčne	159.653	212.567	243.296	272.887	320.666
• bančne	343.521	421.228	415.666	438.823	498.670
• podjetniške	125.391	173.489	178.197	208.993	243.401
• osebne	404.456	515.261	510.145	551.645	629.879
• poslovne	64.456	79.456	83.718	96.171	112.192
debetne		289.301	775.032	961.982	1.392.379

Vir: Šteblaj, 2000, str. 49-56 in http://www.bsi.si.

V splošnem poznamo več vrst plačilnih kartic:

a) Kreditne plačilne kartice

Kreditne plačilne kartice so:
- kartice na odloženo plačilo, pri katerih gre za zamik v poravnavi plačila, ki je bilo opravljeno s tako kartico, poravnava pa se opravi enkrat mesečno, in sicer na določen dan;
- prave posojilne kartice, ki jih izdajajo le banke in pri katerih imetniki lahko poleg odloga plačila koristijo še posojilo banke izdajateljice. To pomeni, da je imetnikom odobreno okvirno posojilo v določeni višini, le-ta pa je odvisna od višine mesečnih prilivov. Imetnik te kartice mesečno odplačuje odstotek zneska porabljenega posojila in pripadajočih obresti.

Konec leta 2000 je bilo izdanih 742 tisoč kreditnih plačilnih kartic (Tabela 2). V tem letu se je število izdanih kartic povečalo za 14% glede na leto 1999. Okoli 60% izdanih kreditnih plačilnih kartic je domačih, torej so jih izdali slovenski izdajatelji in so uporabne v Sloveniji. Okoli 70% vseh izdanih kartic ob koncu leta 2000 so izdale banke kot samostojne izdajateljice ali na podlagi sklenjenih licenčnih pogodb. Glavnina kartic (85%) je bila izdana fizičnim osebam.

S kreditnimi karticami, izdanimi v Sloveniji, je bilo v letu 2000 opravljenih 52 milijonov plačil. Uporaba kreditnih kartic se je glede na leto 1999 povečala za 18% (Tabela 1).

- **Domače in licenčne kreditne kartice**

Domače plačilne kartice (Activa, Karanta) so tiste, ki se uporabljajo za plačila izključno v slovenskem prostoru, in jih izdajajo domači izdajatelji - banke in podjetja. **Licenčne** plačilne kartice (Visa, American Express, Eurocard/Mastercard, Diners Club) je mogoče uporabljati za plačila tako v Sloveniji kot v tujini, izdajajo pa jih domače banke in podjetja na podlagi licenčne pogodbe. To pomeni, da izdajatelji licenčnih kartic s sklenitvijo pogodbe z licenčnim partnerjem pristanejo na pravila poslovanja, ki veljajo za celotno poslovanje s karticami določene blagovne znamke.

Izdaje domačih kartic v Sloveniji presegajo izdajo licenčnih, vendar pri izdajanju licenčnih kartic opažamo nekoliko hitrejšo rast, saj se je število izdanih domačih kartic v letu 2000 povečalo za 12%, število licenčnih pa kar za 18% glede na leto 1999.

Z domačimi plačilnimi karticami je bilo v letu 2000 v Sloveniji opravljenih skoraj 32 milijonov plačil, kar je okoli 60% celotnega prometa s kreditnimi karticami, izdanimi v Sloveniji. Promet je bil za 12% večji kot v predhodnem letu. Promet s karticami, izdanimi na podlagi licence v Sloveniji, ki predstavlja manjši delež, je v letu 2000 glede na predhodno obdobje porasel za 27%.

- **Bančne in podjetniške kreditne kartice**

Bančne kartice izdajajo banke bodisi samostojno (Activa, Karanta, Posojilna kartica Karanta, Kmečka kartica ter kartici HKS in Agrocard) ali na podlagi licenčne pogodbe s tujim partnerjem (kartice iz skupine Eurocard/Mastercard in Visa). **Podjetniške** plačilne kartice, izdajajo podjetja prav tako samostojno (Magna, Mercator Pika kartica, OMV kartica) ali na podlagi licenčnih pogodb (American Express, Diners Club, Euroshell kartica, slednja je uporabna samo v tujini).

V Sloveniji so skoraj 70% kreditnih plačilnih kartic izdale banke; z njimi je bilo v letu 2000 opravljeno tri četrtine prometa glede na celoten promet s kreditnimi karticami.

Bančne in podjetniške kartice se lahko izdajajo tudi kot licenčne kartice. Se pravi, da so izdane na podlagi licenčne pogodbe s tujim izdajateljem ter jih je mogoče uporabljati v Sloveniji in tujini. Pri nas jih izdajajo večinoma banke. Po uporabi kartic v tujini okoli 90% vseh plačil v tujini opravijo imetniki bančnih licenčnih kartic.

- **Osebne in poslovne kreditne kartice**

Osebne plačilne kartice so kartice, ki se izdajajo fizičnim osebam (občanom). **Poslovne** plačilne kartice so kartice, ki se izdajajo podjetjem. Namenjene so vodilnim ali drugim delavcem v podjetjih ali samostojnim podjetnikom, in sicer za plačilo določenih stroškov (potovalni, reprezentančni ...). Za uporabo poslovne kartice se pooblasti eno ali več oseb, ki so zaposlene v podjetju, in se jim določi višina dovoljene porabe na mesec. Med poslovnimi karticami (imetnik je podjetje, uporabnik uslužbenec) so po uporabi v ospredju podjetniške kartice, ki jih izdajajo podjetja (Magna, Diners Club, OMV kartica). Uporaba bančnih poslovnih kartic pa je precej manjša.

Iz podatkov ob koncu leta 2000 je razvidno, da fizične osebe opravijo glavnino prometa s kreditnimi karticami. 85% izdanih kreditnih kartic je bilo osebnih.

b) Debetne plačilne kartice

Debetne kartice (Activa Maestro, BA Maestro Cirrus) so se v Sloveniji prvič pojavile leta 1997, ko so slovenske banke začele postopno zamenjavati čekovne kartice, ki so imele identifikacijsko funkcijo pri plačevanju s čekom in bankomatsko funkcijo, z novimi karticami, ki omogočajo imetnikom še takojšnji (debetni) način poravnave obveznosti na elektronsko opremljenih prodajnih mestih (POS terminali). Ta kartica ni izdana za zagotavljanje potrošniškega kredita, ampak za opravljanje enostavnega brezgotovinskega plačila. Plačilo se izvrši takoj, ko je to mogoče. Odlog plačila, ki nastane pri plačevanju z debetno kartico, je odvisen izključno od (ne)zmogljivosti tehnologije plačilnega sistema.

Z debetnimi karticami je bilo v letu 2000 opravljenih 14 milijonov plačil. Plačila z debetnimi karticami predstavljajo 27% plačil, ki so jih v tem letu opravili imetniki kreditnih kartic. To je tudi razumljivo, saj so imetniki bolj zainteresirani za uporabo kreditnih kartic, ker jim njihova uporaba omogoča odloženo plačilo, medtem ko je pri uporabi debetnih kartic bremenitev

imetnikovega računa takojšnja. Iz tabele 1 in 2 je razvidno povečevanje uporabe debetnih kartic po letih, tako po številu izdanih kartic kot tudi po številu plačil. V prihodnosti je mogoče pričakovati še nadaljnje povečevanje uporabe debetnih kartic, saj se mreža POS terminalov ustrezno širi in izboljšuje se seznanjenost imetnikov z možnostmi uporabe te kartice.

c) Tuje plačilne kartice

Tuje plačilne kartice, ki jih imetniki (pretežno nerezidenti) uporabljajo v Sloveniji, delimo na kartice naftnih družb, ki jih imetniki uporabljajo za nakup goriva na bencinskih črpalkah, kartice drugih podjetij (Diners Club, American Express) in bančne kartice (Visa, Eurocard/Mastercard, Eurocheque Cirrus kartice).

V Sloveniji je bilo v letu 2000 s tujimi plačilnimi karticami opravljenih 3,7 milijona plačil, kar je za 28% več kot v letu 1999. Do večje uporabe tujih plačilnih kartic pride vedno v tretjem četrtletju vsakega leta, kar kaže na prisotnost sezonske komponente - turizma v poletnih mesecih, ki vpliva na večjo uporabo tujih kartic v teh mesecih.

d) Kartice s predplačilom

V Sloveniji obstajajo enonamenske predplačilne kartice z vgrajenim čipom in kartica, ki deluje na radijski frekvenci. Obe vrsti kartic izdajajo podjetja. Poznana je **čip kartica** Telekoma Slovenije, ki predstavlja telefonsko kartico z različnim številom impulzov, s katerimi je mogoče plačevati telefon. Druga kartica - **elektronska kartica**, imenovana Elektronska tablica podjetja Dars za plačilo cestnin, deluje podobno kot čip kartica, vendar na radijski frekvenci. Pri uporabi obeh podjetniških kartic gre za predplačilo storitev, ki jih nudi izdajatelj.

Uporaba elektronske kartice za plačilo cestnin se iz leta v leto povečuje, medtem ko je uporaba telefonskih kartic že začela upadati. Vzrok za to je iskati v velikem porastu mobilne telefonije v Sloveniji.

Ena izmed oblik čip kartic je tako imenovana **elektronska denarnica**, ki pa jo je zaenkrat mogoče uporabljati le v tujini. Te kartice izdajajo predvsem banke in so namenjene za poravnavanje nižjih zneskov plačil (parkirnine, cestnine, nakup časopisov, javni transport itd.).

Kartico je mogoče uporabiti povsod, kjer obstajajo tehnične možnosti sprejema. Napolniti pa jo je mogoče kar na bankomatih.

Razlog za uvajanje pametnih kartic, od katerih naj bi bila elektronska denarnica najbolj množična, in ne klasičnih kartic z magnetnim trakom je, da so bolje zaščitene pred zlorabami in lahko zberejo več informacij. Lastnik elektronske denarnice lahko plačilo opravi zelo preprosto, hitro, gotovine mu ni potrebno nositi s seboj in vedno lahko poravna točen znesek. Za prejemnika plačila pa se z njeno uporabo znižajo oportunitetni stroški zadrževanja gotovine v blagajni. Elektronska denarnica vsebuje predplačilo, zato ni nobene skrbi glede plačnikovega kritja na računu pri banki.

V Sloveniji torej trenutno obstajajo le enonamenske kartice, medtem ko pravih elektronskih denarnic, ki bi jih bilo mogoče uporabljati za poravnavanje plačil v več dejavnostih, še nimamo.

2. 2. Varnost poslovanja s plačilnimi karticami

Varnost poslovanja s karticami je izredno pomembna, saj so zlorabe plačilnih kartic v svetu zelo razširjen pojav, ki povzroča kartični industriji večmilijardno škodo. Popolnih preprečevalnih mehanizmov ni, saj so zlorabe bile in se bodo dogajale tudi v prihodnje. Za zagotavljanje varnosti poslovanja s plačilnimi karticami se uporabljajo metode za zagotavljanje avtentičnosti kartic, za ugotavljanje identitete imetnika kartice, pomembno vlogo ima tudi proces avtorizacije transakcij in obveščanje imetnikov kartic in trgovcev. Novost na področju varnosti predstavljata pametna kartica in SET protokol za varno poslovanje s plačilnimi karticami prek interneta.

a) Avtentičnost kartic

Za zagotavljanje avtentičnosti kartic se pri njihovi izdelavi uporabljajo različni varnostni elementi, ki jih mora vsebovati kartica: mikrotisk, podpisni trakovi, magnetni trakovi, ultravijolični tisk, številka kartice in koda na podpisnem traku, hologrami, embosirni znaki[2] in podobno.

[2]Embosirni znaki so reliefno izbočeni znaki številke kartice,veljavnosti ter imena in priimka imetnika kartice.

Naj kot primer omenim zaščitne znake kartic Visa in Eurocard, ki sta v svetovnem merilu prevladujoči.

- Visa: Na sprednji strani teh kartic je hologram, ki pri menjavanju smeri pogleda kaže zamah golobjega krila. Številka kartic ima bodisi 13 ali 16 številk in se vedno začne s številko 4. Pod ultravijolično svetlobo se v sredini kartice na sprednji strani prikaže leteči golob. Logo Vise na sprednji strani obkrožajo mikročrke. Pri manipuliranju na polju za podpis se pojavi napis VOID.
- Eurocard: Kreditne kartice Eurocard-Mastercard imajo na sprednji strani hologram z globusom, ki iz določenega kota kaže celino. Številka kartice se začne s številko 5. Polje za podpis vsebuje številko kartice in trimestno kodo, ki ni na vseh karticah (Ivanovič, 1995, str. 43).

b) Identifikacija imetnika kartice

Identiteta imetnika kartice se ugotavlja na podlagi primerjave podpisa imetnika kartice na podpisnem traku kartice s podpisom na potrdilu o nakupu. Ta oblika varnostnega mehanizma je s časom izgubila pomen, saj so trgovci prenehali preverjati istovetnost podpisov. Za ugotavljanje identitete imetnika kartice se uporablja tudi osebna identifikacijska številka (PIN - Personal Identification Number), ki nudi višjo stopnjo zaščite, ne pa popolne, saj se PIN lahko pozabi, ukrade, sposodi ali izgubi.

Za varnejšo in učinkovitejšo identifikacijo imetnika kartice so nekateri izdajatelji začeli uvajati kartice s fotografijo imetnika, kar je znižalo število zlorab pri izgubljenih in ukradenih karticah. Izdajatelji imajo o uvedbi teh kartic določene pomisleke, tako da se usmerjajo v še bolj varne načine identifikacije kot je biometrična identifikacija lastnika kartice. Ta način se omenja v povezavi s pametno kartico (glej poglavje 2. 2. 1. Pametna kartica). Za identifikacijo se uporablja prstni odtis, geometrija roke, slikovni vzorec očesne šarenice, glas, podpis. Gre za fizične lastnosti lastnika kartice, ki so znane kot edinstvene vsakemu človeku in enakih ni možno najti pri nobeni drugi osebi. To pomeni, da so biometrične tehnike danes edino sredstvo za varno in resnično osebno identifikacijo. Današnje metode identifikacije so nezadostne, saj povzročajo bankam ogromno škodo v primeru kraje kreditnih in debetnih kartic. Pri biometrični identifikaciji naprava preveri identiteto lastnika in tako breme preverjanja ni več na strani trgovcev, ki so pri opravljanju identifikacije še vedno podvrženi napakam (večina ne prepozna visoko kakovostnih ponaredkov, ne preverjajo istovetnosti podpisov). Biometrija bo

nedvomno zagotovila varno uporabo kartic, vendar bo preteklo še nekaj časa, preden bo v široki uporabi. Do takrat bo človek še vedno najšibkejši člen v verigi za zaščito pred zlorabami.

c) Avtorizacijski proces

Avtorizacija pomeni privolitev za izvedbo zahtevane finančne transakcije s strani izdajatelja plačilne kartice. Z avtorizacijskim procesom se preverja ali je znesek, za katerega se zahteva avtorizacija, v skladu z limiti porabe določene kartice (poraba preko višine določenega limita opozarja na možnost neporavnave obveznosti ali da je bila kartica ukradena, ponarejena, ne da bi se imetnik tega zavedal) in ali je kartica na stop listi, seznamu kartic, katerih imetnikom izdajatelj ne dovoljuje več uporabljati.

Avtorizacija se izvaja, kadar gre za zneske, ki so višji od maksimalnega znesku nakupa, ki ga kupec lahko opravi na prodajnem mestu brez avtorizacije. Zaželjeno bi bilo, da se avtorizacija izvaja za vsak nakup. Problem predstavljajo prodajna mesta, ki niso opremljena s POS terminali in ki uporabljajo papirnate stop liste. Le-te se ažurirajo samo dvakrat mesečno, tako da prihaja do določenega časovnega zamika od izvršitve blokacije do učinkovanja blokacije (odvzema kartice na prodajnem mestu). Tovrstna tveganja so po obsegu zanemarljiva in se s čedalje večjo razširjenostjo POS terminalov zmanjšujejo.

Poslovanje preko on-line POS terminalov zagotavlja visoko stopnjo varnosti in zanesljivosti. Avtorizacija se izvede avtomatsko za vsako transakcijo ne glede na znesek nakupa ter omogoča avtomatsko preverjanje ali je kartica na stop listi. Vsaka blokacija kartice se takoj uvrsti na elektronsko stop listo, tako da je onemogočena možnost njene zlorabe.

Avtorizacijski proces kljub opremljenosti prodajnih mest s POS terminali ne zagotavlja varnosti v primeru zlorab, ki so izvršene še preden izdajatelji kartic prejmejo obvestilo o zlorabi kartice. Največja verjetnost nastanka zlorabe je ravno v času pred prijavo izgube ali kraje kartice ali druge vrste zlorabe, ko izdajatelj še nima možnosti ukrepati z blokacijo kartice. Zato izdajatelji kartic izvajajo kontrolo porabe imetnikov, ki odkrivajo neobičajne vzorce potrošnje posamezne kartice. Temu sledi preverjanje, ali gre za aktivnosti samega imetnika kartice ali za zlorabo.

Avtorizacijski proces je učinkovit v primeru zlorab, ko povzročitelji poskušajo kartico uporabiti po blokaciji. Zato vsi mednarodni izdajatelji za zagotovitev pravočasne blokacije

kartice uvajajo dežurne telefone, ki delujejo vse dni v letu in 24 ur na dan za prijave izgubljenih, ukradenih kartic, saj le-te povzročajo kartični industriji največje izgube.

d) Obveščanje imetnikov kartic in trgovcev

Seznanjanje imetnikov plačilnih kartic s strani izdajateljev preko osebne pošte ali brošur z napotki o varnem poslovanju s kartico (o pravilnem ravnanju s kartico, o varovanju osebne številke, o ravnanju ob izgubi ali kraji kartice) vpliva na zmanjševanje števila zlorab zaradi izgube ali kraje kartic. Za izobraževanje trgovcev pa so kartični izdajatelji poskrbeli tako, da izdajajo priročnike za delo s plačilnimi karticami. Od prodajnih mest se zahteva vrsta varnostnih pravil, in sicer da ugotovijo ponaredek, opravijo identifikacijski postopek, preverijo avtorizacijo nad mejnim zneskom, zadržijo kartico, obvestijo izdajatelja ali policijo. Zato je pomembno, da imajo trgovci ustrezno znanje, ki bo zagotovilo večjo varnost poslovanja s karticami.

2. 2. 1. Pametna kartica

Pametna kartica[3] (Smart Card) je plastična kartica z vgrajenim mikroprocesorjem na čipu, ki se je v svetu prvič pojavila leta 1979, vendar se takrat ni uveljavila zaradi previsokih stroškov, povezanih z njeno proizvodnjo. Razvoj računalniške tehnologije je omogočil, da je cena pametne kartice padla z deset dolarjev na približno dva evra danes. Ob nadaljnji množični proizvodnji bo samo še padala, vendar cene magnetne kartice verjetno še dolgo ne bo dosegla.

Izumitelj pametne kartice (Roland Moreno) se je osredotočil na finančne storitve kot poglavitno smer pri razvoju in razširitvi uporabe pametnih kartic. Pametne kartice naj bi postale vodilni instrument za prenos in razširitev elektronskega poslovanja zaradi lastnosti, kot sta varnost in sposobnost hranjenja podatkov. Kljub temu je bilo uvajanje pametnih kartic na finančno področje dokaj počasno, saj danes pametne kartice za finančne transakcije predstavljajo majhen del skupnega trga, na katerem se uporabljajo. Na finančnem področju je bilo leta 1995 uporabljenih le 4-6% vseh pametnih kartic, medtem ko je bila njihova uporaba na področju telekomunikacij, programov zvestobe in javnega transporta veliko uspešnejša.

[3]Pametna kartica se imenuje tudi čip kartica, procesorska ali inteligentna kartica.

Nekateri izmed možnih načinov uporabe čip kartice na finančnem področju so (Šteblaj, 1999, str. 71):

- kot plačilno sredstvo; pri zamenjavi z običajnimi plačilnimi sredstvi se čip kartica pojavlja kot elektronska čekovna knjižica, elektronski potovalni ček, elektronska denarnica in podobno,
- za dvig gotovine na bančnih avtomatih,
- za plačevanje obveznosti,
- za prenos sredstev od zunanjega vira na kartico (prenos sredstev s tekočega računa v elektronsko denarnico),
- za avtorizacijo dostopov,
- kot elektronski podpis za preverjanje identitete, verodostojnosti in pooblastil prejemnika in pošiljatelja v sistemu elektronske izmenjave podatkov.

Razlog, da so trije kartični operaterji (Europay, Mastercard, Visa) v letu 1995 začeli uvajati plačilne kartice s čipom, je preprost. Magnetni trak na plačilnih karticah se uporablja že približno 30 let in omogoča hranjenje le nekaj številk in besed, pa še te je možno brisati in spreminjati. Informacije na magnetni kartici so slabo zaščitene pred zlorabami, saj je možno enostavno prekopirati zapis s kartice na drugo kartico. Zlorabe so zlasti razširjene v Aziji in ZDA, kjer so organizirani kriminalci osvojili tehnologijo proizvodnje magnetnih kartic in so ponarejene kartice mnogokrat boljše od originalnih ter jih lahko prepoznajo le strokovnjaki. Čip kartice so pred zlorabami bolje zaščitene, lahko zberejo več informacij ter omogočajo varnejše poslovanje bankam in uporabnikom.

Za izdajatelja in uporabnika pametnih kartic je zelo pomembna zaščita podatkov na njej. Zlorabe preprečuje trojni sistem preverjanja. Prvi je ta, da kartica preveri, ali je terminal, prek katerega poteka plačilo, originalen. Drugi je, da terminal preveri pravilnost kartice. Nazadnje se preveri identifikacija imetnika kartice (ali je imetnik kartice tudi njen lastnik), in sicer z uporabo PIN kode. Po nekaj nepravilnih poskusih vnosa identifikacijske številke se kartica sama zaklene. Do zlorabe pametne kartice lahko vseeno pride, če pride do kraje identifikacijske številke, zato se pojavljajo drugačne oblike zaščite. Gre za biometrične tehnike, na primer primerjave prstnih odtisov, geometrije rok, očesne mrežice ali podpisov. Čitalna naprava preveri, če je biometrični podatek na kartici enak temu, kar pokaže uporabnik. Dodatna zaščita je kodiranje informacij, ki potujejo od terminalov do centrale. Samo pooblaščen računalniški sistem, opremljen z ustreznim šifrantom, lahko bere podatke z originalne kartice.

Tehnologija pametne kartice je dovolj zapletena, da močno zmanjša možnost prevare. Vse je odvisno od zmogljivosti čipa in dovršenosti šifriranja, tako da boljših pametnih kartic ni mogoče kopirati.

2. 2. 2. Protokol SET

Visa in Mastercard sta pripravila varen standard za plačevanje s plačilnimi karticami SET - Secure Electronic Transaction (varna elektronska transakcija) preko interneta. Uporaba plačilnih kartic se zaradi SET-a za komitenta ne bo spremenila, bo pa postala zelo varna. Vsa sporočila pri procesiranju transakcij bodo šifrirana in digitalno podpisana, poskrbljeno pa je tudi za ugotavljanje istovetnosti kupca, prodajalca in banke. Uporabniki plačilnih kartic se bodo morali za uporabo SET-a certificirati pri elektronskem notarju. Postopek plačevanja z plačilnimi karticami po standardu SET poteka v prvih petih fazah, zadnje tri faze pa so izven domene standarda (Kovačič, 1997, str. 136):

1. Komitent začne transakcijo tako, da pošlje šifrirano in digitalno podpisano naročilo za blago in številko kartice. Številka kartice je pri celotnem postopku plačevanja šifrirana in za prodajalca ni vidna.
2. Prodajalec pošlje zahtevek za avtorizacijo svoji banki. Banka odšifrira številko kartice.
3. Banka s šifrirano zahtevo preveri veljavnost kartice pri izdajatelju kartice.
4. Izdajatelj potrdi avtorizacijo in potrdilo šifrira in digitalno podpiše.
5. Banka avtorizira transakcijo prodajalcu; avtorizacija je šifrirana in digitalno podpisana.
6. Komitent prejme blago in račun.
7. Prodajalec od banke zahteva plačilo.
8. Prodajalec dobi plačilo.

3. ELEKTRONSKO BANČNIŠTVO

3. 1. Opredelitev elektronskega bančništva

Elektronsko bančništvo lahko opredelimo kot kakršen koli način poslovanja strank z banko, ki je neodvisen od poslovalnic banke in temelji na informacijski tehnologiji in elektronskih medijih. To je širša razlaga elektronskega bančništva, ki zajema bančne avtomate, elektronsko bančništvo prek interneta, telefonsko bančništvo (v živo in avtomatski odzivnik), mobilno bančništvo, kartično poslovanje. Ožja razlaga elektronskega bančništva se nanaša le na storitve, ki jih uporabljamo prek interneta.

Storitve sodobnega elektronskega bančništva morajo zadoščati naslednjim lastnostim: varnost, popolna avtomatizacija storitev, možnost opravljanja storitev od koder koli in kadar koli (24 ur na dan, 7 dni v tednu).

Elektronsko bančništvo se je pojavilo predvsem iz dveh razlogov:

- banke so tako želele odstraniti vrste v bankah, znižati stroške poslovanja in masovne posle prenesti z bančnih okenc, da bi se bančniki lahko posvetili strankam s svetovanjem in zahtevnejšimi bančnimi storitvami;
- želijo ugoditi strankam, ki tako lahko opravljajo bančne storitve doma.

V svetu število uporabnikov elektronskega bančništva počasi narašča. Povečevanje števila uporabnikov je posledica priročnosti takšnih storitev, skokovitega naraščanja uporabnikov interneta in nizkih stroškov transakcij glede na tradicionalni način poslovanja. Vsekakor pa ima število uporabnikov tovrstnega bančništva tudi svoje meje, ki jih postavlja izobrazba. V eni izmed ameriških raziskav (anketirani so bili le uporabniki interneta), bi se pri uporabi elektronskega bančništva počutilo varne le 29% vprašanih. Ta podatek je precej razumljiv, saj je ljudem težko razložiti in razumeti vse vidike varnosti. Zato so uporabniki navedenega bančništva med bolj izobraženimi, saj lažje zaupajo elektroniki, ker jo bolje razumejo.

Kljub temu da je bilo elektronsko bančništvo za svetovno finančno industrijo ena najtežje pričakovanih tehnoloških rešitev, ni doseglo pričakovanj. V ZDA ima elektronsko bančništvo 14,7 milijona uporabnikov, kar je le 12% gospodinjstev. Ta številka je večja v zahodni Evropi, kjer je že 28 milijonov uporabnikov navedenega bančništva. Finančna industrija je že pred 25 leti prestala podobno tehnološko revolucijo, ki jo je sprožila uvedba bančnih avtomatov, saj so tudi takrat porabniki sprva težko sprejeli nov način poslovanja. Kasneje ko so spoznali njegove prednosti, pa je bančni avtomat postal del njihovega vsakdana.

3. 2. Varnostne storitve in tehnološke rešitve

Varnost poslovanja je pri elektronskem bančništvu za banko ključnega pomena. Zato banke temu vprašanju posvečajo veliko pozornost in skušajo zagotoviti najboljšo možno stopnjo zaščite, ki je trenutno dosegljiva. Pri zagotavljanju varnosti sta udeležena tako banka kot komitent. Banka je dolžna postaviti varen sistem, ki komitentu omogoča, da opravlja bančne storitve enostavno in varno. Še tako dobre tehnologije pa so same po sebi ranljive, če se komitenti ne držijo nekaterih pravil. Zato banke namenjajo veliko pozornost ozaveščanju svojih komitentov o pomembnosti varnega hranjenja certifikatov in gesel. Komitentom svetujejo uporabo pametnih kartic kot medija za shranjevanje sredstev za šifriranje (ključev), saj le-ta danes v svetu predstavlja najvišjo stopnjo zaščite.

Pri uvajanju varnostnih rešitev moramo paziti, da te rešitve ne otežijo uporabe storitev in da izpolnjujejo naslednje kriterije (Pepelnjak, Bradeško, 1997, str. 161):

- so cenovno optimalne in enostavno razširljive,
- so za končnega uporabnika nezaznavne (transparentne) in
- so take, da nadaljnje odpiranje omrežij in njihovo medsebojno povezovanje ne ogroža varnosti zasebnega dela omrežja.

Najpomembnejše varnostne storitve, ki bankam omogočajo nadzor varnosti na področju elektronskega poslovanja, so: avtentikacija, avtorizacija, zaupnost, celovitost, nezavrnitev in nadzor pretoka. Rešitve za navedene varnostne storitve omogoča današnja sodobna tehnologija, in sicer gre za postavitev obrambnega zidu, uporabo šifriranja, digitalnih podpisov in digitalnih certifikatov.

3. 2. 1. Varnostne storitve

- Zaupnost

  Zaupnost sporočila (podatka) preprečuje njegovo nepooblaščeno razkritje. Razkritje sporočila, ki potuje preko omrežja, lahko povzroči hude posledice. Edina rešitev je, da tako sporočilo potuje preko omrežja v šifrirani obliki. Šifriranje je funkcija, ki sporočilo spremeni v neberljivo obliko, ki jo lahko prebere le prejemnik z ustreznim dešifrirnim ključem.
- Celovitost

Celovitost sporočila preprečuje njegovo nepooblaščeno spremembo ali uničenje. Sporočilo, ki potuje preko omrežja, ne sme biti spremenjeno s strani tretje osebe, kar zagotovimo z digitalnim podpisovanjem. Digitalni podpis temelji na nesimetričnem šifriranju, in sicer se za šifriranje uporablja pošiljateljev zasebni ključ, za dešifriranje pa njegov javni ključ.

- Avtentikacija

  Avtentikacija zagotavlja prejemniku, da je sporočilo poslal točno določen pošiljatelj in ne morda nekdo drug, ki bi se zanj izdajal, ter da ja sporočilo pristno oziroma ni ponarejeno. Avtentikacijo zagotavljajo digitalni podpis in elektronski notarji z digitalnimi certifikati.

- Avtorizacija

  Pri avtorizaciji gre za nadzor dostopa do določenih informacij. Komitent, ki uveljavlja dostop do informacij, se mora identificirati, da je res subjekt, ki ima pravico do teh podatkov. Običajno se kot sredstvo za avtorizacijo uporablja geslo v kombinaciji z uporabniškim imenom.

- Nezavrnitev

  Nezavrnitev (nezanikanje) preprečuje nepriznavanje katerega izmed udeležencev komunikacije, da je sodeloval v komunikaciji (ne more zanikati, da so poslali oziroma prejeli določeno sporočilo). Digitalni podpis pa je tisti, ki onemogoča zanikanje vsebine poslanega sporočila.

- Nadzor pretoka

  Ukrep za varnost vsakega sistema v omrežju je ustrezno filtriranje, ki ustavi vse tiste, ki dejansko nimajo kaj iskati v varovanem delu omrežja. Preverjajo se naslovi, odkoder sporočilo prihaja ali kamor je namenjeno, njihova vsebina, dostop je omogočen samo pooblaščenim uporabnikom. Ves promet, ki je bil zavrnjen, mora biti zabeležen, saj lahko le tako odkrijemo poskuse vdorov. Nadzor se izvaja v obrambnih zidovih, ki so danes edini varni način povezave zasebnih omrežij z javnimi.

3. 2. 2. Tehnološke rešitve

3. 2. 2. 1. Šifriranje

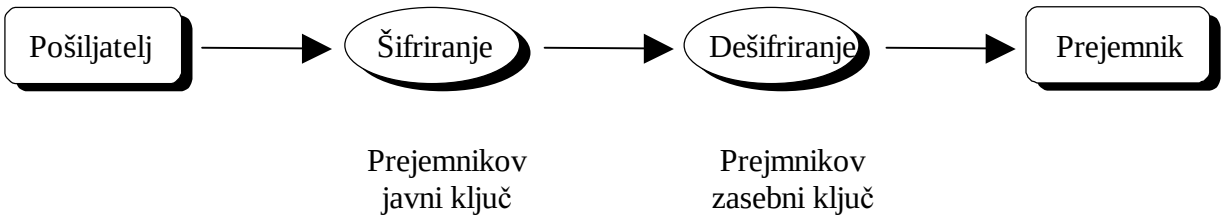
Šifriranje (kriptografija) onemogoča osebi, ki je prestregla šifrirano sporočilo, da iz njega pridobi originalno sporočilo. Šifriranje je torej sprememba sporočila v obliko, ko se ga da prebrati le s pomočjo šifrirnega ključa. Danes sta v uporabi dve obliki šifriranja, in sicer simetrično in asimetrično šifriranje.

Pri **simetričnem šifriranju** je ključ za šifriranje in dešifriranje sporočila enak. Primer simetričnega šifriranja je osebno geslo (številka) pri bančni kartici. Pošiljatelj in prejemnik uporabljata enak ključ (simetrični ključ), ki ga smejo poznati samo osebe, ki so pooblaščene za šifriranje ali dešifriranje določenega sporočila. Poglavitna slabost takega načina je, da moramo imeti za vsakega uporabnika, s katerim želimo varno komunicirati, poseben ključ. Poleg tega pa pri simetričnem šifriranju prejemnik tretjemu ne more neizpodbitno dokazati, kdo je pošiljatelj, kajti prejemnik ima vse šifrirane podatke, s katerimi lahko sporočilo ponaredi (dve osebi imata enaka ključa). Pošiljatelj in prejemnik si morata zaupati in imeti zanesljivo pot za izmenjavo ključa. Če želimo zagotoviti varno komunikacijo, mora biti ključ tudi varno dostavljen udeležencem komunikacije.

Pri **asimetričnem šifriranju** je šifrirni ključ kombinacija zasebnega in javnega ključa. Vsaka banka in komitent posebej imajo za šifriranje podatkov dva ključa, in sicer javni in zasebni ključ. Zasebne ključe se uporablja za dešifriranje podatkov in jih je potrebno varovati, medtem ko se javne ključe uporablja za šifriranje podatkov in morajo biti dostopni vsem. Če želi komitent poslati sporočilo preko omrežja banki, za šifriranje podatkov uporabi javni ključ banke, ki ga lahko dešifrira le banka s svojim zasebnim ključem. V primeru prestreženega sporočila in poznavanja javnega ključa banke nihče ne more priti do vsebine sporočila, razen banke in komitenta, če je izpolnjen pogoj, da sta zasebna ključa komitenta in banke ostalim neznana.

Javni in zasebni ključ sta matematično povezana, tako da sporočilo šifrirano z enim ključem lahko dešifriramo samo z uporabo drugega, vendar zasebnega ključa ni mogoče določiti na podlagi javnega. Prednost nesimetričnega šifriranja je v tem, da je eden izmed ključev javno dostopen, ne da bi bila pri tem ogrožena varnost komunikacije. Seveda je potrebno poskrbeti za verodostojnost javnih ključev pri neodvisnih agencijah. Gre za certifikatne agencije, ki s certifikatom jamčijo, da določen javni ključ zares pripada stranki, s katero komuniciramo.

Slika 1: Asimetrično šifriranje

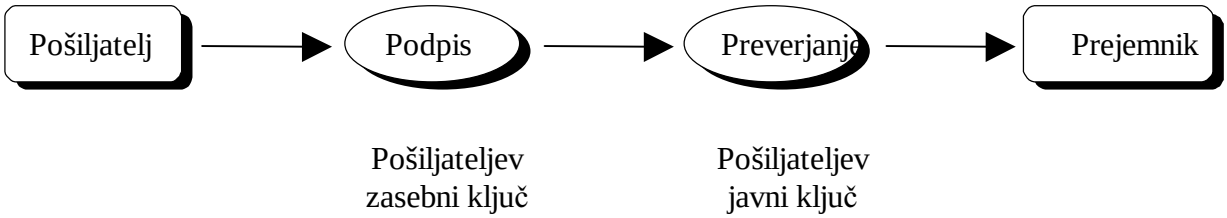


Vir: McKeown, 2001, str. 204.

3. 2. 2. 2. Digitalni podpis

Digitalni podpis se uporablja za preverjanje verodostojnosti pošiljatelja in zagotavlja, da sporočilo, ki potuje med uporabnikom in varovanim sistemom, ni bilo spremenjeno s strani tretje osebe.

Slika 2: Digitalni podpis



Vir: McKeown, 2001, str. 205.

Poslanemu sporočilu preko javnega omrežja dodamo posebej izračunan povzetek[4] (metoda za izračun povzetka je javno znana), ki je šifriran s komitentovim zasebnim ključem, kar imenujemo digitalni podpis. Ko banka prejme šifrirano sporočilo in njegov digitalni podpis, najprej dešifrira podpis s komitentovim javnim ključem (s tem se prepriča, da je bil pošiljatelj resnično ta komitent) in še enkrat izračuna povzetek prejetega sporočila. Če se izračunani in prejeti povzetek ujemata, pomeni, da je sporočilo enako poslanemu (ni bilo spremenjeno) in komitentovo sporočilo odšifriramo z bankinim zasebnim ključem. Komitent svojega podpisa ne more zanikati, saj je bil razkrit z javnim ključem, ki razkrije le njegov podpis (zasebni ključ). Nihče drug ne bi mogel šifrirati sporočila na tak način. V primeru, da se povzetka ne ujemata, je podpis ponarejen ali pa je bilo poslano sporočilo spremenjeno. Ta sistem torej omogoča varno elektronsko podpisovanje dokumentov.

Za zanesljivo delovanje je ključnega pomena varovanje zasebnega ključa. Shranjevanje zasebnega ključa na disku je lahko tvegano, saj ga je možno dokaj preprosto prenesti v drug računalnik. Varnejši način predstavlja hranjenje zasebnega ključa na pametni kartici, saj ključa iz kartice ni mogoče prekopirati. Pametno kartico oziroma dostop do zasebnega ključa je potrebno zavarovati z geslom, ki si ga uporabnik določi sam. Vsak uporabnik je torej zaščiten z nečim, kar ima (pametna kartica in zasebni ključ), in z nečim, kar ve (geslo za dostop do zasebnega ključa).

V primeru, da uporabnik kartico izgubi in jo najditelj poskuša zlorabiti, se kartica samodejno uniči po treh poskusih vpisa napačnega gesla. Težava se pojavi, če je najditelju znano tudi imetnikovo geslo za uporabo kartice. Imetnik pametne kartice s pomočjo zasebnega ključa izvede digitalni podpis, podpis z ukradeno kartico in pravilnim geslom pa je tehnološko pristen podpis. V tem primeru ni mogoče dokazati, da kartice v resnici ni uporabljal njen pravi imetnik. Po Zakonu o elektronskem poslovanju in elektronskem podpisu[5], ki je bil v Sloveniji sprejet junija 2000, je elektronski podpis enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost. Če pa ob izgubi ali kraji pametne kartice ni razkrito tudi geslo, potem do zlorabe ne more priti. Imetnik si lahko priskrbi novo pametno kartico z enakim zasebnim ključem.

Uporabnik lahko uporablja isti par ključev za podpisovanje in šifriranje podatkov. Slednje odsvetujejo iz naslednjih razlogov (Center Vlade RS za informatiko, 2001):

- Zasebni ključ, ki ga uporablja za podpisovanje, sme poznati samo lastnik, saj bi sicer lahko tajil, da je podpisal nek dokument. Torej v nobenem primeru ne sme nihče, razen lastnika, imeti varnostnih kopij tega ključa. Nasprotno pa je za zasebni ključ, ki ga uporablja za dešifriranje, včasih nujno, da ga pozna še kdo drug in da imamo varnostne kopije, saj bi sicer lahko izgubili pomembne podatke.
- Javni ključ, ki pripada zasebnemu ključu za podpisovanje, se mora hraniti tudi po tem, ko ni več veljaven, da lahko preverimo podpise na starih dokumentih. Za javni ključ, ki ga uporabljajo njegovi dopisovalci za šifriranje podatkov, pa to ni potrebno. Ko preneha veljati ali se izgubi, tvori in objavi novega.

[4]Povzetek si lahko predstavljamo kot prstni odtis sporočila, in vsako sporočilo ima drugačnega. Če v sporočilu spremenimo eno samo črko, potem dobimo povsem drugačen povzetek sporočila.
[5]Elektronski podpis označuje vse možne oblike podpisa, dobljenega z elektronsko tehnologijo, medtem ko je digitalni podpis dobljen s pomočjo šifriranja.

- Ni nujno, da imamo za oba para ključev isto obdobje veljavnosti - za par za podpisovanje je to obdobje običajno daljše.

3. 2. 2. 3. Digitalni certifikat

Banka mora preveriti istovetnost komitenta, komitent pa istovetnost banke. Ko nekdo poskuša poslati zahtevo po opravljanju bančnih storitev, banka ne more zagotovo vedeti, če gre res za osebo, za katero se izdaja. Lahko se zgodi, da bi se nekdo lažno predstavil za komitenta banke. Identiteto komitentov in banke zato zagotavljajo elektronski notarji z digitalnimi certifikati.

Certifikatne agencije oziroma elektronski notarji zagotavljajo identiteto komitentov in banke, ki poskrbijo, da se komitenti fizično identificirajo in pri njej shranijo javne ključe. Za komitente lahko elektronski notariat opravlja banka sama, kar pomeni, da sama shrani njihove javne ključe ali pa to prepusti specializiranim ustanovam. Da pa bi komitenti lahko identificirali banko, je potrebno, da se banka identificira pri nekem elektronskem notarju, saj sama ne more jamčiti za svojo identiteto.

V Sloveniji je bil junija 2000 sprejet Zakon o elektronskem poslovanju in elektronskem podpisu, ki določa, da je potrebno za varno elektronsko poslovanje vzpostaviti infrastrukturo t.i. certifikatnih agencij. Certifikatne agencije oziroma overitelji izdajajo digitalne certifikate, ki potrjujejo povezavo med javnim ključem in osebo ali institucijo. Digitalni certifikat vsebuje podatke o imetniku, njegov javni ključ, podatke o izdajatelju potrdila ter obdobje veljavnosti le-tega. Celoten zapis je podpisan z zasebnim ključem izdajatelja certifikata. Overitelj tako predstavlja ustanovo, ki ji zaupajo njeni komitenti (imetniki digitalnih potrdil), hkrati pa s tem zaupajo tudi ostalim uporabnikom potrdil, ki jih je izdal ta overitelj.

Certifikatna agencija lahko izda certifikat samo, če zanesljivo ugotovi identiteto osebe, ki zahteva potrdilo. Uporabljati mora ustrezno zavarovano infrastrukturo za izdajo in hranjenje certifikatov in za shranjevanje svojega zasebnega ključa. Brez popolne varnosti zasebnega ključa overitelja bi bili certifikati popolnoma neuporabni, saj bi jih lahko spreminjal kdor koli. Overitelj lahko izdaja digitalna potrdila na različnih ravneh zaupanja (nižji, srednji, višji). Potrdilu, ki je bilo podeljeno tako, da se je posameznik osebno oglasil in predložil osebni dokument, je mogoče bolj zaupati kot podeljenemu potrdilu na osnovi zahtevka, poslanega po elektronski pošti. Overitelj mora poskrbeti tudi za seznam preklicanih digitalnih potrdil.

3. 2. 2. 4. Požarni zid

Požarne pregrade so varni način povezave zasebnih omrežij z javnimi in jih opredelimo kot sklop naprav in postopkov, ki skrbijo za nadzor in kontroliran dostop uporabnikov v zaščiteno omrežje in iz njega. Požarni (obrambni) zid je filter med zasebnim omrežjem in internetom, ki prepreči dostop do zasebnih omrežij, ki so priključena na internet, če ti uporabniki za to nimajo pooblastil, ter omogoča uporabnikom znotraj obrambnega zidu dostop do interneta. Vsa sporočila gredo mimo obrambnega zidu, ki zavrne sporočilo, ki ne ustreza določenim varnostnim pogojem, in tako ne dovoli vstopa v interno omrežje. Prav tako požarni zid omejuje tudi pošiljanje sporočil iz notranjega v zunanje omrežje (npr. dokumenti, ki so označeni z "strogo zaupno", kar požarni zid zazna in prepreči oddajo takšnega sporočila). Požarni zid registrira število pristopov in število (registriranih) poskusov vdora, saj požarni zid poskusa vdora, ki ga ne more preprečiti, tudi ne more registrirati. Obrambni zid ne more zaščititi omrežja pred prometom, ki je na videz netvegan oziroma njegove tveganosti ne pozna: npr. nekateri obrambni zidovi preprečujejo dostop virusov do omrežja, vendar pa ne morejo zaustaviti virusov, ki jih ne poznajo. Zato je pomembno nenehno nadgrajevati programsko opremo obrambnega zidu.

4. MOBILNO BANČNIŠTVO

4. 1. Mobilno poslovanje

Najnovejša oblika elektronskega poslovanja se imenuje mobilno poslovanje, ki omogoča poslovanje ne glede na čas, kraj ali situacijo, v kateri se uporabnik nahaja. Mobilno poslovanje pomeni, da so ljudje pri svojem poslovanju mobilni in pri tem uporabljajo najsodobnejšo tehnologijo. Seveda mora biti tehnologija tudi prirejena za takšno uporabo (lahka, enostavna za uporabo, delovanje tudi na baterije). Mobilno poslovanje zajema vse, od bančnih storitev, rezervacij in plačila vstopnic, vozovnic, parkirnine, vremenskih podatkov, podatkov o stanju tečajev vrednostnih papirjev do oblikovanja in podpisovanja pogodb, urejanje zavarovanja in razne razvedrilne storitve.

V Sloveniji je že več kot 50% prebivalcev uporabnikov mobilnih telefonov. Kljub temu da je število uporabnikov mobilnih telefonov v svetu že zelo veliko in tudi zelo presega število internetnih uporabnikov, se pričakuje nadaljevanje njihove rasti. Ocenjuje se, da bo evropski trg mobilnega poslovanja narasel s 323 milijonov evrov leta 1998 na 23 milijard evrov leta 2003.

Ljudje radi uporabljamo mobilni telefon, smo ga navajeni uporabljati in imeti vedno s seboj, zato so mobilne storitve precej bolj enostavne in učinkovite kot spletne storitve. Uporabnik je dosegljiv vedno in kjer koli in tudi storitve so vedno dosegljive uporabniku. Mobilne storitve lahko uvedemo na skoraj vsa področja poslovanja in eno od teh je tudi bančništvo. Do leta 2003 bodo najpomembnejši del storitev mobilnega poslovanja predstavljali mobilno oglaševanje (23%), borzno poslovanje, plačevanje in mobilno bančništvo (21%) ter mobilno nakupovanje (15%).

4. 2. Mobilno bančništvo

Mobilno bančništvo omogoča uporabnikom opravljanje bančnih storitev (pregledovanje stanja in prometa na bančnih računih, plačevanje računov, pridobivanje bančnih informacij, tečajnih list, informativnih izračunov ...) od kjer koli in kadar koli z uporabo mobilnih naprav (mobilni telefon, ročni osebni računalniki). V Sloveniji je mobilno bančništvo preko WAP portala prva ponudila SKB banka v povezavi z Mobitelom. Trenutno je komitentom na voljo kot dodaten vir informacij o tečajih, medvalutnih razmerjih in podatkih o banki, mogoče je pridobiti tudi osebne informacije (podatki o stanju in prometu na računu), kasneje pa bo mogoče plačati položnico ali opraviti kakšno drugo storitev. Vse to bomo lahko opravljali zares kadar koli in kjer koli.

4. 2. 1. Kratka sporočila SMS

Gre za sistem kratkih sporočil (SMS - Short Message Service), ki temelji na GSM telefoniji in je doživel nesluten razmah. Storitev kratkih sporočil je bila v Evropi na voljo že leta 1992, vendar pa je do eksplozije uporabe SMS sporočil prišlo šele leta 1999. Oktobra 1999 je bilo poslanih 20 milijard kratkih sporočil v GSM omrežju, s tem da je okoli 90% poslanih kratkih enostavnih sporočil ene osebe drugi, medtem ko so ostalo mobilne informacijske storitve (novice, tečajna lista, vremenska napoved, stanje na cestah ...). Sistem kratkih sporočil je

idealna tehnologija za pošiljanje obvestil uporabnika-uporabniku ali uporabnika več uporabnikom.

Sistem kratkih sporočil omogoča enostavne informativne storitve, ki ne potrebujejo večje varnosti in zaupnosti. Med uporabniki je zelo priljubljeno prejemanje osebnih bančnih obvestil o spremembah na izbranih računih, periodična obvestila o stanju na računu in podobno. Uporabnik si lahko s pomočjo elektronskega bančništva nastavi, kdaj in katera sporočila želi prejemati, ali pa pošlje banki SMS sporočilo, ki vsebuje dogovorjeno ključno besedo, da dobi želeno informacijo. Pomanjkljivost SMS bančnih sporočil je v enosmerni komunikaciji. Izvajanje plačil in drugih storitev s pomočjo SMS sporočil je teoretično izvedljivo, a preveč zamudno. Sporočila, ki so poslana komitentom, morajo biti v šifrirani obliki. V nasprotnem primeru bi to pomenilo, da so ti podatki lahko dostopni morebitnim prisluškovalcem in niti banka niti komitent ne bi mogla ugotoviti, če je zasebno sporočilo prišlo v roke tretji osebi.

4. 2. 2. Protokol brezžičnih aplikacij - WAP

Bančništvo, temelječe na WAP-u (Wireless Application Protocol), ki povezuje mobilno tehnologijo in internet, je ena najnovejših oblik sodobnega bančništva. WAP podpira varno in dvosmerno komunikacijo, zato je primeren za prejemanje javnih in zasebnih sporočil ter za izvajanje plačil. Sistem na osnovi WAP protokola omogoča opravljanje vseh bančnih storitev, od enostavnih informativnih do takih, ki zahtevajo višjo stopnjo varnosti podatkov in identifikacijo uporabnika.

Informacije, dostopne preko mobilnega omrežja, imajo precej omejitev v primerjavi s storitvami preko drugih kanalov (majhni zasloni, nizka hitrost prenosa podatkov ...), zato je WAP protokol oblikovan tako, da deluje znotraj teh omejitev. Seveda pa bistvo mobilnih storitev ni prenos ogromnih količin podatkov. Današnja družba se že tako in tako srečuje z informacijsko preobremenjenostjo. Zato je pomembno uporabniku ponuditi informacijo, ki mu nudi določeno korist, tako da mu je zares na voljo samo gola in zanj pomembna informacija oziroma vsebina.

4. 2. 2. 1. Delovanje prototipne rešitve mobilnega bančništva

Splošne bančne informacije, informativni izračuni in tečajne liste so na voljo vsem uporabnikom brez prijave v sistem elektronskega bančništva. Za pregled stanja, prometa in za plačevanje računov se je potrebno najprej prijaviti v sistem. Uporabnik mora vpisati osebno številko in geslo. Če oboje vpiše pravilno, ga sistem pozdravi z izpisom imena in priimka. Za pregled stanja je iz menuja potrebno izbrati *Stanje* in račun, za katerega želimo izpis. Izpiše se številka računa, stanje na računu, datum zadnje spremembe in limit. Pregled prometa za izbrani račun pokaže znesek, namen in datum ter ali je znesek v dobro ali breme. Za plačevanje računov je iz menuja potrebno izbrati *Plačila.* Prikažejo se možnosti: *Nov račun* ali pa računi, ki so bili plačani že kdaj prej. Pri računih, ki so bili že plačani, so že izpolnjeni vsi podatki. Uporabnik, če želi, spremeni določene podatke, kot so znesek, namen in datum plačila. Potem pa izvede plačilo. Če uporabnik plačuje nov račun, mora vnesti vse podatke, ki jih zahteva storitev. To so: izbrati račun, s katerega želi plačati, vpisati znesek, namen, naziv prejemnika, račun prejemnika in sklic. Vnesene podatke mora uporabnik še preveriti in potrditi izvedbo plačila. Po izvedbi se na zaslonu izpiše potrdilo, da je bil račun uspešno plačan (Hribar, 2001, str. 241).

4. 3. Varnost mobilnega bančništva

Stopnjo varnosti bančnih storitev lahko priredimo glede na tveganje, ki se pojavlja pri posamezni storitvi (ali gre samo za pregled stanja, plačevanje, višino zneska, ki se pri storitvi obdeluje). Mobilno bančništvo se pri vgrajenih varnostnih mehanizmih v precejšnji meri zgleduje po elektronskem bančništvu in zraven ponuja še nekaj dodatne zaščite, kot je pametna kartica SIM (Subscriber Identity Module), ki zagotavlja overjanje lastnika. S tem je zagotovljena višja stopnja varnosti, kot je navadno za fiksno internet omrežje. Poleg tega je mobilni telefon namenjen za osebno uporabo in ga načeloma ne delimo z drugimi uporabniki.

SIM kartica omogoča avtentikacijo uporabnika, saj se za vsako identifikacijsko številko skriva točno določen uporabnik. Uporabnik lahko aktivira kartico samo s PIN kodo. Po trikratnem napačnem vnosu omenjene kode se kartica blokira in zahteva PUK kodo (Personal Unblocking Key), ki ob desetkratnem napačnem vnosu povzroči trajno blokacijo kartice.

Za zagotovitev večje varnosti je možno, da se na SIM kartici oblikuje za prejemanje SMS bančnih sporočil poseben meni "bančništvo", in se ne uporablja standardni SMS meni v aparatu. Dostop do posebnega menuja je možen samo z osebno tajno številko, s čimer se

dodatno potrdi identiteta uporabnika. Menu se po določenem času samodejno izklopi in aktivira PIN, če v tem času ne zazna nobene aktivnosti.

Problem varne brezžične komunikacije je, da obstoječe SIM kartice zaradi premajhne kapacitete ne morejo sprejeti šifrirnih algoritmov in formatov certifikatov. Prenos podatkov po mobilnem omrežju je zakodiran. Ključi za kodiranje so krajši od tistih, uporabljenih v elektronskem bančništvu, a so še vedno zanesljivi. Obojestransko overjanje je nujni pogoj za mobilno bančništvo. Uporabnik mora biti prepričan, da komunicira z banko, banka pa, da komunicira s točno določenim uporabnikom. Rešitev predstavljajo digitalni certifikati, ki pa so preobsežni in jih ni mogoče shraniti na SIM kartici. Prav tako mobilni telefoni niso zmožni sprejeti oziroma preveriti certifikata, ki ga pošlje banka. Brez podpore digitalnim certifikatom pa ni mogoče izpeljati dovolj varnega mobilnega bančništva. Do takrat so bančne storitve, dostopne preko mobilnih telefonov, obsojene bolj na informativno kot finančno dejavnost.

V okviru WAP protokola je shranjevanju digitalnih certifikatov že namenjen dodatni identifikacijski modul WIM (Wireless Identity Module). Njegova naloga je:
- da izvaja kriptografske operacije,
- generira par ključev (zasebnega in javnega) ali pa se ta par ključev naloži nanj ob oddaji naprave lastniku,
- hrani zasebni ključ,
- generira zahtevek za podpis javnega ključa ter shrani digitalno potrdilo, ki ga dobi od overitelja,
- digitalno podpisuje,
- opravi vse potrebne operacije za izmenjavo skupnega ključa za šifriranje podatkov.

Pri shranjevanju digitalnih potrdil, ki vsebujejo javne ključe, je več možnosti:
- hrani se v WIM-u, kar je tudi najbolj učinkovito,
- tu se lahko shrani le naslov (URL) strani, kjer je digitalno potrdilo shranjeno
- ali pa ga strežnik dobi kako drugače.

Identifikacija uporabnika in vzpostavljanje varne povezave potekata v več korakih:

- Digitalni certifikat uporabnika se ob njegovi identifikaciji prenese na strežnik, ki ga ta brez težav preveri.
- Strežnik pošlje uporabniku svoj digitalni certifikat z javnim ključem. Strežniki naj bi uporabljali preprostejše certifikate, ki bi bili manj obsežni in bi jih lahko mobilni telefon sprejel. Življenjska doba takšnih certifikatov naj bi bila omejena le na nekaj dni, saj ne ustrezajo varnostnim merilom.
- Da bi se uporabnik prepričal o veljavnosti certifikata, kontaktira s seznamom preklicanih certifikatov.
- Ko se uporabnik prepriča o verodostojnosti strežnika, mu pošlje t.i. "session key" oziroma enkratni ključ, ki je generiran za vsako povezavo posebej. Ta ključ je zašifriran s strežnikovim javnim ključem (da ne more priti v napačne roke) in podpisan z uporabnikovim zasebnim ključem (s tem se dokaže, da gre za točno določenega uporabnika).
- Zašifriran enkratni ključ strežnik dešifrira s svojim zasebnim ključem in preveri uporabnikov podpis. Sedaj lahko uporabi enkratni ključ za vzpostavitev varne povezave oziroma za šifriranje podatkov.

Asimetrično šifriranje (javni in zasebni ključ) je precej počasno in ravno zato naj bi se uporabljalo v kombinaciji z enkratnim ključem. Le-ta je razmeroma kratek, tako da je šifriranje podatkov s pomočjo tega ključa hitro (uporabnik in strežnik za šifriranje in dešifriranje podatkov uporabljata enak ključ, t.j. enkratni ključ).

S šifriranjem se zagotovi zaupnost in celovitost podatkov pri prenosu preko mobilnega omrežja. V primeru asimetričnega šifriranja je javni ključ dostopen vsakomur, zasebni pa je spravljen na kartici in ga ni možno ukrasti, prekopirati ali kako drugače zlorabiti. Za celovitost podatkov dodatno poskrbi digitalni podpis, katerega namen je tudi zagotavljanje avtentičnosti in nezanikanja. Na ta način bi bile izpolnjene vse varnostne zahteve.

4. 4. Mobilno plačevanje po svetu

Ponudniki storitev po vsej Evropi so spoznali, da je mobilni telefon lahko nadvse priročno plačilno sredstvo. Kljub temu spoznanju je pravzaprav zelo malo že delujočih sistemov, ki bi omogočali, da uporabniki kot plačilno sredstvo uporabijo kar svoj mobilni telefon namesto gotovine ali kreditne kartice. Najdlje so na tem področju prišli v finski Soneri in v Španiji.

Trije španski operaterji mobilne telefonije so združili moči z dvema največjima bankama in ustanovili družbo Mobipay, katere cilj je čim bolj spodbuditi razvoj mobilnega plačevanja v Španiji. Sistem Mobipay nastaja že dve leti in naj bi začel delovati v začetku leta 2002. Za prihodnje uporabnike bo plačevanje enostavno in bodo za plačevanje računov s pomočjo mobilnega telefona, uporabljali svoje že dosedanje račune pri bankah. Plačevanje bo omogočeno na prodajnih avtomatih in na klasičnih blagajnah.

Kako uporabnik takšno plačilo doživi v praksi? Na blagajni povemo številko mobilnega telefona ali posebno geslo, če ne želimo izdajati svoje številke, ali celo črtno kodo, nalepljeno na telefon. Zatem na ekranu mobilnega telefona prejmemo informacijo o nakupu, vključno s ceno. Nazadnje nakup samo še potrdimo z vpisom 5-mestne PIN kode (kakršno bomo v prihodnosti uporabljali za vse tovrstne transakcije).

V finski Soneri (Sonera Mobile Pay) so se odločili za drugačno pot. Njihovi uporabniki lahko že nekaj časa plačujejo z mobilnim telefonom na približno 500 prodajnih avtomatih različnih vrst (avtopralnice, izposojevalnice videokaset, avtomati z napitki in prigrizki). V primeru avtopralnice uporabnik pošlje kratko sporočilo SMS, ki vsebuje ključno besedo, na številko, ki je zapisana na avtopralnici. Uporabnik prejme potrdilo o bremenitvi računa, številko računa in posebno kodo. Enako kodo prejme tudi blagajna avtopralnice in služi kot dokazilo, da je bila storitev plačana preko SMS-a. Znesek opravljenega nakupa pa se prišteje uporabnikovemu telefonskemu računu. Ta način plačevanja se je odlično prijel in prodaja se je na prodajnih avtomatih, kjer so uvedli to plačilno metodo, povečala za 20 do 30 odstotkov. Kljub začetnim uspehom na področju prodajnih avtomatov pa so rešitve za plačevanje z mobilnim telefonom na klasičnih blagajnah še v razvojni fazi.

Razvoj mobilnih storitev je šele na začetku. Lahko samo slutimo neskončne možnosti, ki nam jih bodo v prihodnosti omogočili mobilni operaterji skupaj s ponudniki storitev. Vsekakor je prihodnost v mobilni tehnologiji.

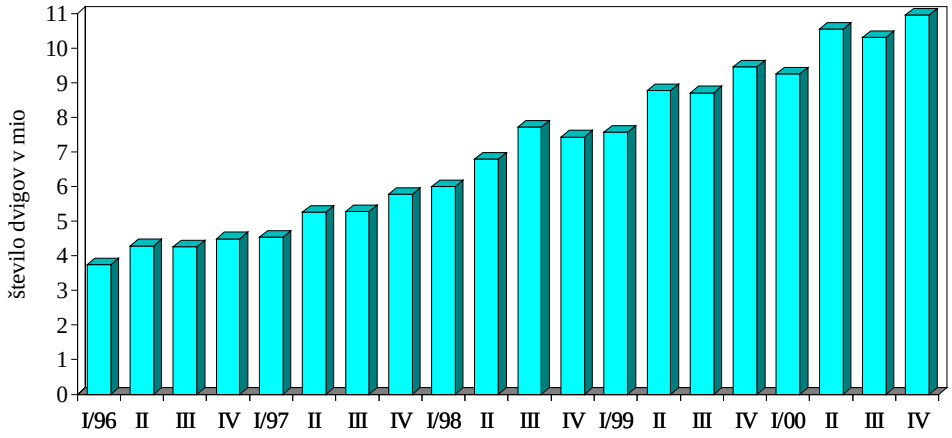
5. BANČNI AVTOMAT

Leta 1968 je britanska Barclays Bank dala v uporabo prvi samopostrežni bančni avtomat, sledile so ji druge banke v Veliki Britaniji in ZDA, z manjšo zamudo pa tudi banke drugje po svetu. Začetki poslovanja prek bančnih avtomatov v Sloveniji segajo v leto 1990.

5. 1. Bančni avtomati v Sloveniji

Bančni avtomati so samopostrežni terminali, povezani z računalnikom. Z njihovo pomočjo lahko komitenti opravijo enostavna bančna opravila brez prisotnosti bančnega delavca. Prvotno so bili namenjeni le izdaji gotovine, sčasoma so prerasli v avtomate za poslovanje s plačilno-kreditnimi karticami, plačevanje računov in pologov na bančne račune, kar jih označuje za transakcijske avtomate. V prihodnosti bi se iz njih lahko razvili različni modeli. Bankomat bi lahko predstavljal informacijsko okno, kjer bi bil komitent povezan s spletnimi stranmi, preko infoterminalov bi se odvijale predstavitve in oglaševanje. Predstavljal bi prodajno okno, kjer bi bil komitent povezan s podjetji. Le-to bi bilo mesto za prodajo znamk, kinematografskih kart, letalskih, železniških in avtobusnih vozovnic, mesto za plačilo dohodnine, plačilo raznih obveznosti na račune podjetij itd. (Tomassini, 1999, str. 40-41).

Slika 3: Uporaba bančnih avtomatov[6] v Sloveniji po četrtletjih od leta 1996 do 2000



Vir: Šteblaj, 2000, str. 60 in http://www.bsi.si.

Iz Slike 3 je razvidno, da se uporaba bančnih avtomatov po četrtletjih v Sloveniji povečuje. V letu 2000 je bilo 41 milijonov dvigov z bančnih avtomatov, kar je za 19% več kot leta 1999.

[6] Bančni avtomati so obravnavani le z vidika gotovinske funkcije, čeprav nudijo še vrsto drugih storitev.

Povprečni znesek dviga na bančnih avtomatih se skozi leta povečuje, in sicer z 8.917 tolarjev v letu 1999 na 10.354 tolarjev v letu 2000.

Uporaba bančnih avtomatov je posledica prednosti, ki jih le-ti nudijo bančnim komitentom. Bankomati so dostopni 24 ur na dan in vse dni v tednu, tako da komitenti opravijo določene storitve, ko imajo čas in niso vezani na delovni čas bančnih enot. Izognejo se tudi čakanju pred bančnimi okenci. Poleg tega je uporaba bankomatov zelo enostavna in hitra. Edina omembe vredna slabost bančnih avtomatov je neoseben odnos, kar povzroča, da starejši ljudje zelo malo uporabljajo bančne avtomate in raje stojijo pred bančnimi okenci, kot da bi prešli na enostavnejši in hitrejši način poslovanja z banko.

5. 2. Varnost poslovanja preko bančnih avtomatov

Kot sem že omenila, je bančni avtomat samopostrežni terminal, povezan z nekim glavnim oziroma matičnim računalnikom, preko katerega potekajo vse transakcije, ki se izvajajo preko bankomata. Bančni avtomat ima zelo dober samodiagnostični sistem za odkrivanje napak in težav v lastnem delovanju (napake v strojni opremi bankomata, programski opremi, zmanjka papirja, gotovine). Takrat to sporoči glavnemu računalniku in prekine svoje delovanje, v primeru ropa in nesreč pa se tudi zaklene. Seveda je opremljen z alarmnim sistemom zaradi možnosti vlomov.

Za varnost uporabnikov oziroma za varnost poslovanja preko bankomatov so odgovorni predvsem uporabniki. Poslovanje z bančnim avtomatom je za uporabnika zelo enostavno, saj ga skozi ves postopek vodi bankomat sam. Na njegovem ekranu se sproti izpisujejo navodila za nadaljevanje postopka. Za varno poslovanje preko bančnih avtomatov je bistvenega pomena uporaba osebne identifikacijske številke (PIN - Personal Identification Nubmer), s katero se imetnik kartice identificira. Zato je potrebno skrbeti za njeno ustrezno varovanje. Bančni avtomat kartico odvzame, če večkrat pride do napačnega vnosa osebne identifikacijske številke, in s tem onemogoča njeno uporabo nepooblaščenim osebam. Odvzame tudi neveljavne in blokirane kartice.

Pravilnost oziroma nespremenjenost prenosa zahtevane transakcije se preveri na podlagi kode za varovanje neokrnjenosti sporočila (MAC - Message Authentication Code). Le-ta je izračunana že na bančnem avtomatu s pomočjo izmenjevalnega ključa, ki se menja vsakih

petnajst minut. Izmenjevalni ključi skrbijo za kodiranje sporočil in transakcij ter jih poznajo le bančni avtomat in centralna aplikacija. V primeru, da MAC koda ni pravilna, je prišlo do napake pri prenosu ali zlorabe transakcije, tako da se transakcija zabeleži in zavrne. V primeru, ko se postopek nadaljuje, se transakcija preveri po različnih kriterijih (aktivna kartica s pravilno serijsko številko, blokacija, datumska veljavnost, dnevni limit ipd.) in se zapiše na magnetno stezo kartice ter v bazo aktivnih kartic.

Zlorabe pri poslovanju preko bančnih avtomatov so predvsem posledica malomarnosti imetnikov kartic pri varovanju PIN številk, saj prihaja največkrat do zlorab zaradi ukradenih ali izgubljenih kartic, ki so imele v bližini tudi PIN. Najvišjo stopnjo varnosti bodo v prihodnosti nedvomno predstavljali bankomati, kjer bo dostop temeljil na biometrični identifikaciji (npr. identifikacija roženice, glasovna identifikacija). V Veliki Britaniji ima Barclays Bank trenutno v fazi testiranja uporabo bankomatov na osnovi biometrije (slikovni vzorec šarenice). V ZDA 650 bankomatov uporablja za identifikacijo prstni odtis uporabnika skupaj s pametno kartico. Samo biometrija zagotavlja zanesljivo identifikacijo uporabnika, saj se PIN še vedno lahko pozabi, ukrade, sposodi ali izgubi.

Od težav, ki se pojavljajo v zvezi z bankomati, je najbolj pogosta ta, da uporabnik pozabi vzeti gotovino. Rešitev za omenjeni problem predstavlja vgrajena kaseta za zadržane bankovce, v katero gre gotovina, če jo uporabnik pozabi vzeti. Problem je v tem, da se to zgodi šele po pol minute, v tem času pa jo že lahko naslednji uporabnik pospravi.

6. TELEFONSKO BANČNIŠTVO

6. 1. Opredelitev telefonskega bančništva

Telefonsko bančništvo omogoča opravljanje bančnih storitev po telefonu in deluje na dveh različnih pristopih do komitenta, in sicer prek avtomatskega telefonskega odzivnika in prek bančnega operaterja. Telefonsko opravljanje bančnih storitev je primerno za vse, ki nimajo računalnika oziroma jim v tem trenutku ni na voljo, pa bi radi poslovali na daljavo.
Telefonski odzivnik je naprava, ki se z vnaprej pripravljenim posnetkom samodejno odzove na klic uporabnika. S pritiski na telefonsko številčnico uporabnik usmerja delovanje telefonskega odzivnika in tako pridobi splošne ali zasebne informacije. Avtomatski telefonski odzivnik

neznanim uporabnikom daje splošne informacije o bančni ponudbi, menjalniških tečajih tujih valut, obrestnih merah itd. Znanim bančnim uporabnikom pa posreduje informacije, ki so osebne narave, kot npr. stanje in promet na računu, naroči čeke, plača položnice, veže tolarske in devizne depozite itd.

V imenu klicočega bančni operater izvede različne negotovinske bančne storitve, vključno s plačili po predhodni identifikaciji uporabnika. Bančnik v skladu z našimi navodili računalniško izvede naročeno transakcijo (poišče podatke o stanju na računih, podaljša izredni limit, podaljša vezavo sredstev ...). Delovanje bančnega operaterja dopolnjuje telefonski odzivnik in ga tako razbremeni pogostih klicev z vprašanji o stanju na računu. Telefonskega bančništva se stranke poslužujejo najpogosteje ravno z namenom, da sprašujejo o stanjih na računih.

Hitrost in praktičnost sta razloga, zaradi katerih se stranke odločajo za uporabo telefonskega bančništva. Stranke najpogosteje uporabljajo telefon za preverjanje stanja na računu. V ZDA v 40 odstotkih primerov stranke sprašujejo o stanjih na računu (podobno je v Veliki Britaniji), 30% predstavlja poizvedovanje o dospelosti čekov, denarnih transakcij je 12%, medtem ko je bančnih prodaj (kot so npr. krediti) le okoli 3%. V Belgiji banke beležijo 80% klicev z željo po informacijah, ostalo pa so klici z željo po denarnih transferjih.

6. 2. Varnost telefonskega bančništva

Pri opravljanju bančnih storitev preko telefona se identificiramo s pomočjo identifikacijske kartice. Identifikacijska kartica generira časovno spremenljivo varnostno geslo, ki ga komitent uporabi ob prijavi. Vsako geslo je uporabno samo enkrat. Identifikacijska kartica je zaščitena z osebno identifikacijsko številko, ki jo pozna le uporabnik, saj jo v identifikacijsko kartico vnese sam po lastnem izboru pred prvo uporabo kartice. Iz varnostnih razlogov se vsi razgovori, vezani na opravljanje bančnih storitev, snemajo in hranijo na zavarovanem mestu, da ni skrbi pri morebitni potrebi po potrdilih o plačilih računov.

Za varno identifikacijo komitenta se uporablja tudi načelo PIN/TAN. PIN je osebno geslo, ki ga pozna le uporabnik in s katerim je mogoče izvajati opravila, ki se nanašajo na specifičnega uporabnika, ne potrebujejo pa njegovega podpisa. Gre predvsem za informacije, kot so stanje na računu, pregledi prometa idr. Za izvajanje opravil, ki jih mora komitent tudi podpisati, je poleg PIN-a potrebno uporabiti še transakcijsko (podpisno) kodo - TAN

(TransActionNumber), ki nadomešča lastnoročni podpis. Komitent prejme od banke serijo TAN kod, vsaka koda pa je uporabna samo enkrat. Ko komitent večino porabi, dobi novo serijo. V primeru, da uporabnik trikrat zaporedoma vnese napačno osebno geslo ali podpisno kodo, mu je nadaljnja uporaba storitev onemogočena.

7. ČEK

7. 1. Uporaba čeka v Sloveniji

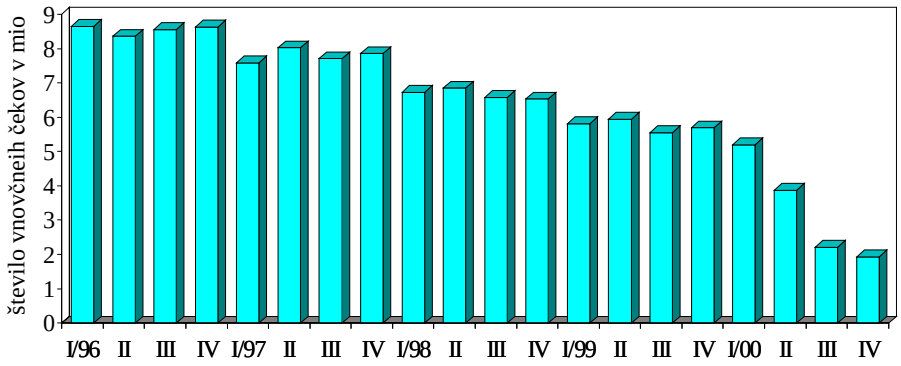
Ček je 250 let star instrument plačilnega prometa, ki je preskušen, uzakonjen in zato ponuja sodno varstvo. Prestal je različne družbene ureditve in zato ga lahko uvrstimo v svetovno zakladnico instrumetnov plačilnega prometa.

Ček je nepogojni nalog komitenta (trasanta), dan banki (trasatu), da v breme dobroimetja, katerega ima komitent pri banki, banka plača čekovnemu upravičencu (remitentu) določen denarni znesek. Uporablja se v plačilnem prometu znotraj države in tudi zunaj njenih meja ter omogoča plačilo brez prenašanja in izročanja gotovine. V našem pravu se ček lahko trasira le na banko kot trasata.

Uporaba čeka[7] kot plačilnega instrumenta se zmanjšuje. V letu 2000 je bilo v Sloveniji unovčenih 13 milijonov čekov občanov, kar je za 43% manj kot v preteklem letu. Vzroke za njegovo zmanjševanje je možno pripisati uveljavitvi debetne funkcije čekovne kartice in porastu uporabe kreditnih plačilnih kartic. Uporaba čekovne kartice v plačilni funkciji nadomešča predvsem uporabo čeka zaradi enostavne uporabe in večje varnosti poslovanja. Uporaba čeka se zmanjšuje tudi zaradi omenjenega porasta uporabe plačilnih kartic, poleg tega pa banke računajo na še večjo uporabo plačilnih kartic, saj od 1. julija 2000 unovčujejo remitentom le tiste čeke, ki imajo kritje na trasantovem (izdajateljevem) tekočem računu.

[7]Število plačil s čeki je lahko manjše od števila unovčenih čekov, saj lahko posamezno plačilo s čekom pomeni unovčitev večjega števila čekovnih blanketov, ker je znesek, ki ga lahko unovčimo s posameznim blanketom, omejen.

Slika 4: Uporaba čeka v Sloveniji po četrtletjih od leta 1996 do leta 2000



Vir: Šteblaj, 2000, str. 45 in http://www.bsi.si.

Čekovne kartice so lahko izdane brez ali s PIN kodo, slednje prevladujejo. Kartice s PIN kodo so namenjene poslovanju na elektronsko opremljenih prodajnih mestih (plačilna funkcija čekovne kartice) in omogočajo uporabo bančnega avtomata. Čekovne kartice brez PIN kode imajo le identifikacijsko funkcijo pri plačevanju s čekovnimi blanketi, so torej namenjene identifikaciji plačnika oziroma avtorizaciji izdanih čekov. Uporabljajo se tudi kot dokazilo o jamstvu bank za izplačilo vsakega čeka do določene vrednosti.

7. 2. Vrste čekov

Po načinu določitve čekovnega upravičenca ločimo:

1. *Ček na ime* vsebuje natančno označbo čekovnega upravičenca, t.j. remitenta čeka, ki je lahko fizična ali pravna oseba.
2. *Ček na prinositelja* vsebuje klavzulo plačajte prinositelju.
3. *Lastni trasirani ček* je ček, pri katerem sta trasant in trasat ista oseba.
4. *Ček, trasiran po lastni odredbi,* kjer sta trasant in remitent čeka ista oseba.

Po namenu ločimo:

1. *Gotovinski ček* je ček, s katerim trasant izda nalog trasatu za izplačilo določenega denarnega zneska remitentu v gotovini .
2. *Prenosni ček* je ček, s katerim trasant da banki nalog, naj z njegovega računa prenese določen denarni znesek na račun remitenta.
3. *Obračunski ček* vsebuje klavzulo samo za obračun, s katero se prepoveduje gotovinsko izplačilo.

4. *Bariran ček* (vsebuje dve diagonalni črti) je unovčljiv samo pri določeni banki in je lahko splošen ali poseben z označbo določenega trasata.

Posebne vrste čekov:

a) *Certificiran ček*

S certifikacijo čeka banka potrjuje, da je do višine certificiranega zneska blokirala kritje na trasantovem računu ter da se obvezuje ta znesek čekovnemu upravičencu plačati.

b) *Ček z vizo*

Z viziranjem čeka banka potrjuje obstoj čekovnega kritja v času izdaje čeka, vendar sama ne prevzema obveznosti, da bo ček ob predložitvi v plačilo tudi plačala.

c) *Bančni ček*

Bančni ček je ček, pri katerem se banka pojavlja kot čekovni trasant (izdajatelj) in trasat. Za predložitev bančnega čeka v plačilo velja rok šestih mesecev od dneva izdaje čeka.

7. 3. Varnost poslovanja s čeki

Zaradi pomembnosti funkcije, ki jo opravlja ček, ter zaradi ohranjevanja zaupanja vanj, čekovni zakon določa denarne kazni za kršitev določil Zakona o čeku. Zakon o čeku pa kršijo tako trgovci kot trasanti. Trasanti kupujejo različno blago na obroke, tako da trgovcem izročijo večje število čekov brez datuma. Ob zapadlosti posameznega obroka trgovci vpišejo datum izdaje čeka in ga takrat unovčijo v banki. Izdajatelj čeka tako prekrši Zakon o čeku, ki prepoveduje, da se ček trasira brez datuma ali z neresničnim datumom izdaje. Trgovec, ki sprejema take čeke, nelojalno konkurira drugim.

Za zagotovitev varnega poslovanja s čekom je pomembno, da mu ne manjka eden ali več bistvenih elementov, da je na računu trasanta dovolj sredstev, da je ček pravočasno predložen na unovčenje ter skrbno varovanje čekovnih blanketov in čekovne kartice:

a) pravilno izpolnjen ček

Zakon o čeku predpisuje šest bistvenih elementov, ki so pogoj za veljavnost čeka, in sicer:

- označbo, da gre za ček, napisano v samem besedilu listine,
- nepogojni nalog, naj se plača določena vsota denarja iz trasantovega kritja,

- ime tistega, ki naj plača (trasat),
- kraj, kjer je treba plačati,
- navedbo dneva in kraja izdaje čeka,
- podpis tistega, ki je ček izdal (trasanta). Pri poslovanju s čeki je potrebno opraviti primerjavo podpisa trasanta na čeku in čekovni kartici v trenutku, ko je ček predložen v plačilo, in sicer mora biti ček podpisan v navzočnosti remitenta. Banka ni dolžna plačati čeka, če je remitentu mogoče očitati malomarnost pri primerjavi podpisa.

Zaradi nepravilnega izpolnjevanja čekovnih blanketov je bilo v Sloveniji v letu 1999 zavrnjenih za 13% več čekov kot leto poprej. Skupna vrednost zavrnjenih čekov je v letu 1999 znašala 46,5 milijona tolarjev, kar predstavlja 0,02% vrednosti unovčenih čekov v letu 1999.

Remitenti, ki sprejemajo plačilo s čekom, morajo biti pozorni na to, da je pravilno izpolnjen, sicer banka takega čeka ne bo izplačala in hkrati kot tak ne nudi nobene varnosti (tveganje nepravilno izpolnjenega čeka).

b) izstavitev čeka s kritjem

Ob izdaji čeka mora imeti trasant pri trasatu čekovno kritje v denarju. Za izdajo nekritega čeka je odgovoren trasant (tisti, ki je ček izdal), nikdar pa nista to niti remitent, ki prejme ček kot plačilo za svoje blago ali storitev, niti banka, saj izplačilo čeka opravi po nalogu in v breme čekovnega dobroimetja trasanta.

Izdaja čeka brez kritja je v številnih državah kaznivo dejanje. Kazenske sankcije so zelo stroge, saj je ček listina javnega zaupanja. Kazenski zakonik nekdanje SFRJ je določal za tistega, ki izda nepokrit ček, zaporno kazen do treh let. V Republiki Sloveniji se za tistega, ki izda ali da v promet ček brez kritja in tako pridobi premoženjsko korist, predvideva zaporna kazen do petih let. V primeru, da je pridobljena velika premoženjska korist, se predvideva zaporna kazen do osmih let.

Trasat, ki izda ček brez kritja, mora dati imetniku čeka popolno odškodnino. Gre za izostalo plačilo in trasant je dolžan imetniku plačati čekovni znesek, zamudne obresti in drugo škodo, ki jo je imetnik čeka utrpel zaradi nepravočasnega plačila.

Ček mora plačati banka, na katero je ček trasiran, vendar je ta obveznosti odvezana, če na računu trasanta ni kritja. Zakon o čeku remitentu v tem primeru omogoča, da pri sodišču vloži protest zaradi izdaje neplačanega čeka ali na podlagi protesta proti remitentu vloži tožbo. Ček je instrument, ki od trasanta zahteva polno zavedanje odgovornosti, če ga izda brez kritja.

Tveganje neobstoja kritja je manjše pri certificiranem čeku, ki ga ni mogoče preklicati in je zagotovljeno plačilo, ter pri bančnem čeku, ki je varen plačilni instrument, seveda če gre za prvovrstno banko.

c) predložitev čeka na unovčenje
Ček je plačilni in ne kreditni instrument in zato ne vsebuje roka dospelosti, temveč je plačljiv ob vpogledu, to je ob predložitvi v plačilo.

Zakon o čeku predpisuje rok, ki se šteje od dneva izdaje, v okviru katerega je potrebno ček predložiti v plačilo, in sicer:
- 8 dni, če je kraj izdaje in kraj plačila čeka isti,
- 15 dni, če je kraj izdaje in plačila čeka različen, vendar v isti državi;
- 20 dni za ček, izdan v drugi evropski državi;
- 40 oziroma 70 dni za ček, izdan v državi zunaj Evrope.

Za bančni ček omenjeni prezentacijski roki ne veljajo. Le-ta se lahko predloži v plačilo v roku šest mesecev od dneva izdaje.

d) varovanje čekovnih blanketov in čekovne kartice
Komitent mora čekovne blankete in čekovno kartico hraniti na tak način, da bo preprečil izgubo, neupravičen odvzem ali zlorabo čekov. Ček je sredstvo za negotovinsko plačevanje in se pri njegovem hranjenju terja enaka pazljivost kot pri hranjenju gotovine. V primeru, ko pride do kraje čekovnih blanketov in je trasant pravočasno obvestil banko o tem, mora banka (trasat) odkloniti vsakršno izplačilo iz trasantovega kritja. Zaradi izgube, kraje čeka, zaradi praznih čekovnih blanketov so najbolj nevarni čeki na prinositelja, saj lahko tak ček unovči kdorkoli, tudi tisti, ki ga slučajno najde.

8. PRIMERJALNA ANALIZA DEJAVNIKOV VARNOSTI

Varnost opravljanja transakcij s plačilnimi karticami, poslovanja s čeki, uporabe telefonskega bančništva, bančnih avtomatov, mobilnega in elektronskega bančništva bom primerjala med seboj po naslednjih kriterijih: identifikacija, zaupnost, celovitost in nezanikanje. Le ob izpolnitvi teh štirih zahtev lahko govorimo o obstoju varnosti pri uporabi sodobnih plačilnih instrumentov. Še tako dobre tehnologije, ki zagotavljajo izpolnjevanje navedenih kriterijev, so neučinkovite, če se uporabnik ne drži določenih "pravil igre". Prav uporabnik sam si je lahko največja nevarnost. Vsekakor mora biti stopnja varnosti uporabe instrumentov takšna, da ne otežuje, upočasnjuje njihove uporabe ali povečuje stroškov. V nasprotnem primeru banke ne bodo pritegnile komitentov k povečani uporabi sodobnih plačilnih instrumentov.

Za ocenjevanje varnosti sem torej uporabila naslednje kriterije:

- Identifikacija: Identifikacija komitenta v transakciji zagotavlja, da je transakcijo izvedel točno določen komitent in ne morda nekdo drug, ki bi se zanj izdajal.
- Zaupnost: Vsako sporočilo oziroma podatki, ki potujejo od komitenta do banke oziroma vsebina transakcije, ne smejo biti razkriti nepooblaščenim osebam.
- Celovitost: Transakcija, ki jo izvede komitent med prenosom do banke, ne sme biti nepooblaščeno spremenjena (okrnjena ali kakorkoli popačena).
- Nezanikanje: Nezanikanje udeležbe v transakciji pomeni zaščito pred tem, da komitent kasneje ne more lažno zanikati, da je opravil določeno transakcijo.

Pomen posameznega kriterija v sklopu vseh kriterijev je lahko različen. Menim, da je največjo težo moč pripisati kriteriju identifikacije, vendar brez izpolnitve tudi vseh ostalih kriterijev varnega poslovanja ni mogoče doseči.

Za izpolnitev kriterija identifikacije se uporabljajo različni mehanizmi, med katerimi obstajajo razlike v stopnji varnosti, ki jo nudijo.

- Najenostavnejši in najmanj varen način identifikacije je identifikacija z uporabniškim imenom in geslom. V zvezi s to obliko identifikacije se pojavljajo problemi, kot so npr. pozabljena in ukradena gesla ali razkrita gesla zaradi slabega varovanja.
- Srednjo zanesljivo stopnjo varnosti nudi koncept PIN/TAN. Za sisteme, ki zahtevajo visoko varnost, je to vsekakor premalo.
- Za zagotovitev visoke stopnje varnosti se lahko uporabi identifikacijska kartica. Le-ta je v obliki kreditne kartice, ki vsako minuto tvori novo geslo (uporabnik ga prepiše z minizaslona), potrebno za dostop do sistema. Vsako posamično geslo je uporabno samo enkrat. Uporaba identifikacijske kartice je zavarovana s PIN-om, ki ga pozna le uporabnik.

V primeru izgube ali kraje identifikacijske kartice ali številke PIN, identifikacijske kartice ne more uporabljati nihče brez številke PIN, ki jo pozna le uporabnik. Če pa je kdo videl PIN, ga ne more uporabljati brez kartice, ki je v uporabnikovi lasti.

- Visoko stopnjo varnosti zagotavlja tudi identifikacija uporabnika s pomočjo digitalnega certifikata na pametni kartici. Dostop do kartice ja zavarovan z osebnim geslom, ki si ga izbere in vpiše uporabnik sam. Uporabnik je zaščiten v primeru izgube ali kraje take kartice, saj se le-ta uniči po treh poskusih vpisa napačne osebne številke.
- Najvišjo stopnjo varnosti nudi biometrija, saj gre za identifikacijo na podlagi neponovljivih bioloških značilnosti posameznika. Uvajanje biometrije predstavlja za banko izredno visok strošek. Vsekakor pa tudi biometrija ni vsemogočna, saj ni primerna za uporabnike-invalide, ki bi se tako lahko počutili še bolj diskriminirane.

Zavedati se moramo, da stoodstotne varnosti pri poslovanju s sodobnimi plačilnimi instrumenti ni mogoče zagotoviti. Zlorabe so bile in se bodo dogajale tudi v prihodnje, verjetno pa jih bo vedno manj in z manjšo škodo. Banke in ostali sistemi morajo zagotoviti, da so sodobni plačilni instrumenti tehnično zelo izpopolnjeni, seveda pa je potem od goljufa in njegove domiselnosti odvisno, kako se bo lotil določene zadeve in poskusil zlorabiti varnostne mehanizme.

a) Elektronsko bančništvo

Pri elektronskem bančništvu je tehnologija javnih ključev osnova za moderno digitalno varnost. Temelji na trojici informacij, ki jih tvorijo uporabnikov zasebni in javni ključ ter digitalno potrdilo. S pomočjo te tehnologije je mogoče ugotavljati in dokazovati istovetnost pošiljatelja in prejemnika, šifriranje podatkov med prenosom po javnem omrežju in omogoča digitalni podpis. Za zagotovitev najvišje stopnje varnosti je pomembno, da se certifikat in zasebni ključ hranita na pametni kartici. V pametni kartici teče majhen program, katerega naloga je le šifrirati, dešifrirati in podpisovati podatke. Pametna kartica nikoli ne izda zasebnega ključa, ampak z zasebnim ključem samo podpisuje podatke. Dostop do pametne kartice je zaščiten z PIN-om. Elektronsko bančništvo zadovoljuje vse kriterije za varno poslovanje (identifikacija, zaupnost, celovitost, nezanikanje).

Pri elektronskem bančništvu si je najbolj nevaren uporabnik sam, saj je na njem breme, da zagotovi varnost v smislu varovanja pametne kartice in številke PIN. V praksi so najpogostejše kraje slabo varovanih sredstev zaščite, in sicer se dogaja, da imajo uporabniki svoje PIN kode

zapisane na listku, ki je nalepljen kar na računalniškem ekranu. Seveda je zloraba v omenjenem primeru zelo preprosta.

b) Bančni avtomat

Tako kot elektronsko bančništvo tudi bančni avtomat izpolnjuje vse kriterije za varno poslovanje z njim. V podjetju Bankart, ki upravlja bankomate, zatrjujejo, da je varnost pri opravljanju transakcij prek bankomatov zelo visoka. Uporaba bankomata je zaščitena s poznavanjem osebne številke - PIN. Če imetnik svoje osebne številke ne da drugi osebi, potem ni nevarnosti. Pomembno je, da si osebno geslo zapomnimo in ga nikoli nimamo zapisanega. Zlorabe na tem področju so precej redke in do njih praviloma pride le zaradi neskrbnega ravnanja z osebno številko. Najvišjo stopnjo varnosti bodo predstavljali bankomati z biometrično identifikacijo. Postavlja pa se vprašanje, ali je uvajanje biometrije stroškovno upravičeno. Danes je varnost poslovanja prek bančnih avtomatov, tako kot pri elektronskem bančništvu, v veliki meri odvisna od uporabnika samega.

c) Telefonsko bančništvo

Varnost uporabe telefonskega bančništva je manjša od elektronskega. Pri telefonskem bančništvu sta izpolnjena kriterija identifikacije uporabnika in nezanikanja, ne pa tudi kriterija zaupnosti in celovitosti. Po telefonu lahko kdor koli prisluškuje pogovoru med komitentom in bančnim uslužbencem, kar pomeni, da zaupnosti ni. Prav tako ni izpolnjen kriterij celovitosti, saj lahko pride do prekinitve telefonske linije in transakcija ostane nedorečena. Pri telefonskem bančništvu je varnost v veliki meri odvisna tudi od uporabnika, torej od njegovega načina varovanja sredstev za identifikacijo.

d) Mobilno bančništvo

Na področju varnosti elektronskega bančništva predstavlja visoko stopnjo varnosti t.i. infrastruktura javnega ključa, ki jo oblikuje sistem šifriranja, digitalnih podpisov in digitalnih certifikatov. Trenutno se še oblikuje rešitev v smeri implementacije tega sistema tudi na področje mobilnega bančništva. S tem bodo tudi izpolnjeni vsi kriteriji (identifikacija, zaupnost, celovitost, nezanikanje) za varno poslovanje. Seveda je tudi pri mobilnem bančništvu, kakor pri

drugih oblikah sodobnih plačilnih instrumentov, varnost njegove uporabe v veliki meri odvisna tudi od samega uporabnika.

e) Plačilna kartica

Tudi pri poslovanju s plačilnimi karticami je bistvenega pomena skrbno varovanje kartice. Pri poslovanju s plačilnimi karticami je kriterij identifikacije uporabnika sicer izpolnjen, vendar trgovci vse redkeje primerjajo podpis na slipu[8] s podpisom na kartici. Prav tako ni izpolnjen kriterij zaupnosti, saj ni zagotovljena varnost podatkov s kartice (podatki s kartice ne bi smeli biti nepooblaščeno razkriti) in lahko samo pričakujemo od trgovca, da ne bo zlorabil podatkov na njej. Vsekakor so plačilne transakcije s karticami bolj varne in cenejše kot pa poslovanje s starejšo obliko brezgotovinskega poslovanja s čeki.

Na kaj moramo biti uporabniki pozorni pri plačilnih karticah za zagotovitev varnosti (I. M. S., 1998, str. 13)?

- Kartica naj bo spravljena na varnem mestu. To običajno ni denarnica, ki jo nepridipravi najprej zmaknejo iz naših žepov. Predvsem na počitnicah jo imejmo vedno pri sebi ali v hotelskem sefu. Če jo pogrešimo, o tem takoj, ampak res isti trenutek, obvestimo banko.
- Kartice nikoli ne spustimo izpred oči. Ko plačujemo, naj operacije opravljajo pred nami. Če plačujemo v restavraciji, ne dovolimo, da natakar izgine z njo v ozadje lokala. V tem primeru je do zlorabe zelo kratka pot.
- Kartičnih slipov (potrdil) nikdar ne zavrzimo. Skrbno jih spravimo, saj zavrženi slipi lahko pridejo v neprave roke. Nekdo bi lahko izdelal kartico z našimi podatki in izropal naš račun. Če nič drugega, za evidenco porabe so potrdila nujna.
- Pri banki povprašamo o zavarovanju kartice pred zlorabo in se seveda odločimo zanj, če nam banka to omogoča.

f) Ček

Plačilne kartice so v Sloveniji že dodobra izpodrinile poslovanje s čeki, ki jih občani v glavnem uporabljajo le še kot obliko kreditiranja na več obrokov. Ček in tudi plačilna kartica z vidika varnosti nekako nista primerljiva z ostalimi instrumenti, ampak med seboj, ker pri ostalih instrumentih omogoča izpolnjevanje kriterijev tehnologija. Poleg tega je potrebno poudariti, da

se npr. od elektronskega bančništva zahteva veliko večja stopnja varnosti kot od čeka, saj se v primeru elektronskega bančništva potencialni kriminalec "lažje skrije" in ga je praviloma tudi težje odkriti.

Identifikacija uporabnika na podlagi primerjave podpisa na čeku in čekovni kartici (podpis izdajatelja čeka mora biti istoveten podpisu na čekovni kartici) se le redko izvaja. Pri poslovanju s čekom ni izpolnjen kriterij zaupnosti in celovitosti. Uporabnik mora čekovne blankete in čekovno kartico skrbno varovati, najbolje na ločenih mestih, če se želi izogniti zlorabi. Kljub neizpolnjevanju navedenih kriterijev za varno poslovanje je čekovno poslovanje nemoteno potekalo dolga leta. Poleg tega je ček velikokrat tudi edini primerni plačilni instrument, ko na primer nimamo na voljo dostopa do računalnika, telefona ali bančnega avtomata.

Glede na to, da se uporaba čeka pri nas zmanjšuje, menim, da ček postopno zapušča kategorijo sodobnih plačilnih instrumentov. Zamenjujejo ga instrumenti, ki so enostavnejši, hitrejši, varnejši in ugodnejši.

[8]Slip je potrdilo o nakupu, ki je sestavljeno iz dveh delov: originalni podpis kupca ostane trgovcu, kupec pa dobi kopijo.

Tabela 3: Primerjava varnosti uporabe sodobnih plačilnih instrumentov

Plačilni instrument / Kriterij	**Elektronsko bančništvo**	**Telefonsko bančništvo**	**Bančni avtomat**	**Mobilno bančništvo**	**Plačilna kartica**	**Ček**
Identifikacija	digitalni certifikat ali identifikacijska kartica	identifikacijska kartica ali PIN/TAN	PIN, v prihodnosti biometrija	digitalni certifikat, SIM kartica	primerjava podpisov, v prihodnosti pametna kartica z biometrijo	primerjava podpisov na čeku in čekovni kartici
Zaupnost	Šifriranje		kodiranje	šifriranje		
Celovitost	digitalni podpis, šifriranje		MAC koda	digitalni podpis, šifriranje	slip (potrdilo o nakupu)	
Nezavrnitev	digitalni podpis	pogovori snemajo in hranijo	evidenca na magnetni stezi kartice in v bazi aktivnih kartic	digitalni podpis	lastnoročni podpis na slipu	lastnoročni podpis na čeku

9. ZLORABE

9. 1. Zlorabe plačilnih kartic

Pri poslovanju s plačilnimi karticami največji delež izgub pri Visi predstavljajo zlorabe zaradi izgubljenih in ukradenih kartic (60%), sledijo izgube zaradi ponarejenih kartic (20%), izgube kartic po pošti - vlomi v nabiralnike, kraje s pomočjo poštarjev in podobno - (10%), ostalo gre pripisati drugim vzrokom. Pri Eurocardu je delež škode zaradi ponaredkov okoli 40%, s tem da je približno 80% ponarejanj v zvezi z zlato kartico[9].

V Sloveniji se izdajatelji plačilnih kartic v največjem obsegu soočajo z zlorabo kartic s strani samih imetnikov, in sicer gre za neporavnave obveznosti imetnikov kartic. Dolžnike lahko razvrstimo v tri skupine (Ivanovič, 1995, str. 44):
- tisti, ki so plačilno sposobni povrniti dolg, vendar so se trenutno iz različnih razlogov znašli v finančni stiski;
- tisti, ki poznajo sistem poslovanja s karticami in prek kreditiranja nakupov poskušajo špekulirati in namerno odlašajo poravnati dolg toliko časa, da bi prek morebitne naložbe kupljenega blaga finančno pridobili;
- tisti, ki zaradi lahkomiselnosti zabredejo v večje dolgove in sploh niso več sposobni povrniti dolga.

Kazenski zakonik Republike Slovenije predvideva za osebe, ki uporabijo bančno kartico na bančnem avtomatu za dvig gotovine, čeprav vedo, da nimajo pokritja, ali uporabijo kreditno kartico, čeprav vedo, da ob plačilu ne bodo imeli pokritja in si bodo tako pridobili premoženjsko korist, zaporno kazen do 5 let. Za vsakogar, ki pridobi znatno premoženjsko korist zaradi zlorabe bančne ali kreditne kartice, pa zakon predvideva do 8 let zapora.

9. 2. Zlorabe interneta

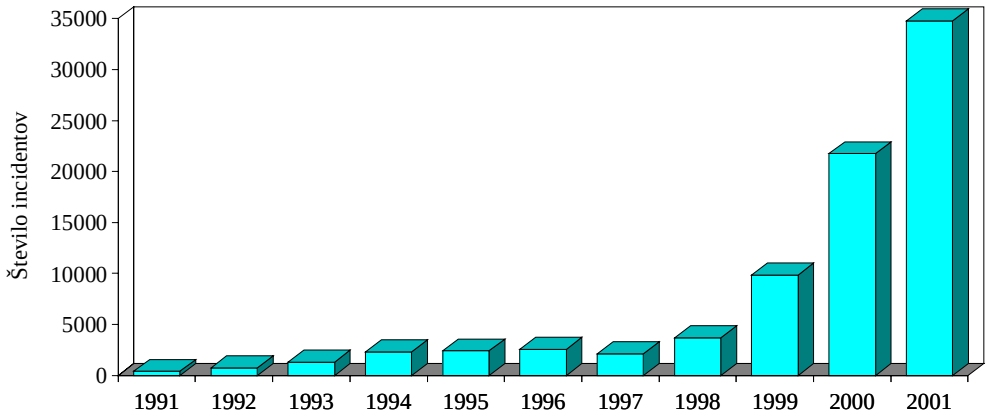
CERT/CC (Computer Emergency Response Team/Coordination Centre) od leta 1988 zbira podatke o računalniških vdorih in zlorabah ter svetuje podjetjem, kako lahko te težave odpravijo. Število incidentov na internetu narašča, saj je izvajanje zlorab preko interneta

najcenejše v primerjavi z drugimi metodami. Še vedno pa ostaja veliko incidentov neprijavljenih, ker se podjetja bojijo, da bodo s tem k vdiranju privabila še druge vdiralce, da bi izgubili ugled in zaupanje pri porabnikih ali pa preprosto zato, ker niso opazili vdorov in kraje podatkov.

Oblike incidentov na internetu so zelo različne. Skupni cilj vseh oblik je bodisi okoriščanje z informacijami, dokazovanje ali povzročanje škode. Ko govorimo o incidentih na internetu, torej mislimo na kakršno koli obliko aktivnosti v povezavi z omrežjem z negativnimi posledicami za varnost, in sicer gre lahko za:

- vdore v sistem, ki imajo lahko za posledico le nepooblaščen dostop do podatkov in njihovo krajo, lahko pa tudi spremembo ali uničenje podatkov,
- prestrezanje sporočil, kjer napadalec ne vdre v sistem sam, temveč za dostop do podatkov uporabi prenosne poti, kjer z ustrezno opremo prisluškuje ali spreminja podatke, ki potujejo po napadeni poti,
- onemogočanje uporabe storitev - tu napadalec poskuša poslabšati kakovost storitve ali jo povsem onemogočiti (npr. z izjemno povečanim številom zahtev po določeni storitvi na sistemu, ki pod tako obremenitvijo ne deluje več optimalno),
- povzročanje stroškov, kjer napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen, kar napadenemu povzroča nepotrebne stroške, druge škode ponavadi nima.

Slika 5: Število incidentov na internetu med leti 1990 in 2001[10]



Vir: CERT/CC, 2001.

[9]Imetnikom zlatih kartic je omogočeno plačevanje visokih zneskov. Pogoji za njihovo pridobitev so strožji ter odvisni od ugleda in rednih prihodkov imetnikov.

Iz slike 5 je razvidno, da število incidentov na internetu z leti narašča. Potrebno pa je poudariti, da je bilo v začetku devetdesetih let, ko je bilo število incidentov še zelo nizko, tudi število uporabnikov interneta in prometa opravljenega preko interneta nizko. V skladu z razširjenostjo interneta torej narašča tudi število incidentov.

9. 3. Zlorabe plačilnih kartic na internetu

Pri poslovanju s plačilnimi karticami preko interneta je lahko stopnja zlorabe od 20-50% od vseh opravljenih transakcij preko interneta. Do zlorab prihaja, ko kriminalci postavljajo lažne spletne strani, ki oponašajo tiste, ki jih imajo legitimni trgovci, in ponujajo neverjetno nizke cene za plačila s kreditnimi karticami. Te spletne strani v resnici ničesar ne prodajajo, temveč je njihov namen samo pridobiti veljavne številke kreditnih kartic. Le-te potem prodajo drugim, ki jih imajo namen zlorabiti ali pa jih uporabijo sami za nakup pri legitimnih trgovcih. Za odpravo takih in podobnih zlorab je bil razvit SET. Protokol SET se uveljavlja precej počasi, predvsem zaradi svoje kompleksnosti in stroškov, povezanih z njegovo vpeljavo.

V začetku prodaje prek interneta se je pojavljala še ena oblika zlorabe. Na vsaki plačilni kartici je dolgo, 13- ali 16-mestno število. Ta številka seveda ni naključna, ampak določena s posebno formulo, ki je drugačna za vsako podjetje, ki izdaja kartice. Tako na primer prve štiri ali pet številk označujejo banko, ki je izdala kartico. Na žalost pa obstajajo programi, s pomočjo katerih lahko ustvarimo 13- ali 16-mestno številko, ki je sicer lažna, a tega brez dodatnega preverjanja ni mogoče ugotoviti. Če dodatnega preverjanja (ali je številka resnična) ni ali ga je mogoče zaobiti, ponarejevalec lahko začne uživati. Ta oblika zlorabe je bila mogoča predvsem ob začetkih prodaje prek interneta, medtem ko je danes dodatno preverjanje nekaj samoumevnega (Mesarič, 2001, str. 12).

Do potrebnih informacij je mogoče priti tudi z vdori v računalnik, ki hrani podatke o imetnikih in številkah plačilnih kartic. Možnost zlorabe je zelo majhna, če podjetje takšne podatke hrani na računalniku, ki ni povezan z internetom. Medtem ko se možnost zlorabe zelo poveča, če jih hrani na istem računalniku, ki sprejema naročila in je povezan v internet (npr. spletne trgovine). Visa in številni drugi ponudniki plačilnih kartic so sprejeli sklop minimalnih standardov, ki jih morajo spoštovati ponudniki blaga in storitev preko interneta. Gre za nadzor in spremljanje

[10]Podatki o številu incidentov na internetu za leto 2001 se nanašajo le na prve tri kvartale.

dostopov do informacij, uporabo enkripcije, vzpostavitev požarnega zidu, varno uničevanje podatkov, ki jih ne potrebujejo več, zaščito pred virusi, redno testiranje varnostnih sistemov in podobno.

Zaradi uporabe tehnologije za kodiranje prenosa je najtežji in najredkejši primer zlorabe prestrezanje informacij, ki potujejo od kupčevega računalnika do strežnika podjetja. Gre za pretvorbo podatkov v tako obliko, da za morebitnega prisluškovalca ni uporabna.

9. 4. Zlorabe pri elektronskem bančništvu

Cilj zlorabe pri elektronskem bančništvu so lahko tako uporabniki kot tudi banka. Pri uporabnikih je najbolj verjetna kraja sredstev zaščite. To pomeni, da nekdo ukrade pametno kartico ter ugotovi PIN za dostop do digitalnih certifikatov. Uporabniki morajo varovati svoja sredstva zaščite podobno, kot varujejo svoje osebne dokumente ali kreditne kartice. Pogosta je kraja certifikata, če je le-ta na trdem disku računalnika in ni varovan z geslom. Pri uporabnikih je možen tudi vdor prek računalniških virusov, ki poskušajo ukrasti PIN kode za dostop do sredstev zaščite. Zato je pomembno, da imajo uporabniki ustrezno protivirusno zaščito, da ne odpirajo sumljive elektronske pošte ali nameščajo različne nelicenčne programe. V praksi so najpogostejše kraje slabo varovanih sredstev zaščite, in sicer se dogaja, da imajo uporabniki svoje PIN kode zapisane na lahko odkritem mestu (na monitorju ali tipkovnici oziroma pisalni mizi). Pot do zlorabe je v omenjenem primeru zelo preprosta.

Cilji napadov so tudi strežniki na bančni strani, na katerih se shranjujejo zaupne informacije, zato je pomembna vrhunska zaščita le-teh pred zunanjimi vdori. V bankah sproti opravljajo pregled prometa prek požarnega zidu v lokalno omrežje. Občasno se sicer pri nas pojavljajo primeri, ko skuša kdo ugotoviti možne vhode v notranje omrežje, vendar so bili vsi dosedanji poskusi neuspešni.

SKLEP

Plačilne kartice so sodobnejši način plačevanja, ki nam že dolgo ni več tuj. Njihova prednost je predvsem v tem, da se izognemo pisanju čekov (njihova uporaba se pri nas postopno zmanjšuje) in plačevanju z gotovino. S karticami odpadejo tudi težave, kako priti do denarja, ko so bančne ustanove zaprte. V Sloveniji smo jih začeli uporabljati že v šestdesetih letih, resničen razmah pa so doživele šele v zadnjem desetletju.

Po načinu izvajanja bančnih storitev največji delež v Sloveniji predstavljajo osebni obiski banke (44,7%), sledi uporaba bankomata (44,4%), medtem ko elektronsko bančništvo (0,8%), telefonsko (0,6%) in mobilno bančništvo (0,02%) predstavljajo še zelo nizke deleže. Mobilno bančništvo se v glavnem uporablja za vpogled v stanje na računu, medtem ko pri elektronskem bančništvu že preko 60% uporabnikov na ta način izvaja tudi transakcije.

Bančni avtomati, elektronsko in telefonsko bančništvo so se v Sloveniji pojavili v devetdesetih letih, z mobilnim bančništvom pa smo se prvič srečali v letu 2000 prek SMS sporočil. Z uvedbo WAP protokola se na področju mobilnega bančništva obetajo velike spremembe in verjetno bodo v prihodnosti ravno mobilni telefoni osnovno sredstvo za vsakovrstno bančništvo. Mobilno bančništvo je tehnološko zelo zahtevno in ustrezne stopnje varnosti ni mogoče zagotoviti brez podpore digitalnim certifikatom. Tehnologije, ki bi to omogočile na cenovno sprejemljiv način, se šele razvijajo. Mobilno bančništvo bo zato še kakšno leto ali tudi več omejeno zgolj na pregled prometa in stanj.

Osnovni pogoj za večjo razširjenost navedenih sodobnih plačilnih instrumentov je zaupanje potencialnih uporabnikov in tudi določeni tehnični predpogoji (npr. osebni računalnik za elektronsko bančništvo, mobilni telefon za mobilno bančništvo ...), česar pa določeni segmenti komitentov nimajo (upokojenci, ljudje z nizkim standardom ...). Zaupanje je pogojeno z zagotovitvijo ustrezne ravni varnosti pri opravljanju transakcij. Prenizka raven varnosti lahko uporabniku povzroči veliko denarno škodo, medtem ko je previsoka raven varnosti povezana z visokimi stroški na strani banke. Ustrezno stopnjo varnosti ne more zagotoviti le uporaba najsodobnejše tehnologije, saj je še vedno potrebno ozaveščati uporabnike in jih v skladu z uporabljeno tehnologijo tudi ustrezno izobraževati. Uporabnik mora torej skrbno varovati svoja sredstva zaščite, saj se pogosto dogaja, da je za zlorabo kriv ravno uporabnik sam. Zelo

pomembno je tudi sledenje novi tehnologiji in sprotno posodabljanje celotnega varnostnega sistema.

LITERATURA

1. Aleksič Milojka: Tudi vaš mobilni telefon je lahko telefonska banka. Bančnik, Ljubljana, 2000, december, str. 8-9.
2. Bem Slavko: Čeki - ali jih bomo še uporabljali?. Bančni vestnik, Ljubljana, 49(2000), 6, str. 1.
3. Blažič-Jerman Aleksej: Banka v žepu. Moj mikro, Ljubljana, 16(2000), 7/8, str. 70-72.
4. Bračun Franc: Praktične izkušnje pri uvajanju elektronskega bančništva. Zbornik: Banke in tveganja. Portorož: Zveza ekonomistov Slovenije, 1997, str. 149-153.
5. Cepec Miro: Elektronsko bančništvo in druge oblike bančništva na daljavo v Sloveniji. Kapital, Maribor, 11(2001), 259, str. 47-48.
6. Chapman D. Brent, Zwicky D. Elizabeth: Building Internet Firewalls. Debastopol: O'Reilly & Associates, 1995. 517 str.
7. Eržen Boris: Digitalno overjeno. Kapital, Maribor, 11(2001), 261, str. 54-55.
8. Eržen Boris: Kako varno je spletno bančništvo. I&T, Ljubljana, 1 (2001), 10, str. 7-11.
9. Fabijan Jane: Vloga centralne banke pri razvoju plastičnega denarja. Bančni vestnik, Ljubljana, 44 (1995), 4, str. 28-31.
10. Falatov Peter: Plačila v mednarodnem poslovanju. Ljubljana: Ekonomska fakulteta, 1999. 204 str.
11. Greganovič Branko: Analiza plačilnih sistemov. Gospodarski vestnik, Ljubljana, 44 (1995), 26, str. 63.
12. Ham Lara: Mobilno plačevanje po svetu: Mobilno plačevanje med Helsinki in Madridom. Motim?, Ljubljana, 2001, 2, str. 8.
13. Hribar Uroš: Storitve mobilnega poslovanja. Organizacija, Kranj, 34 (2001), 4, str. 236-244.
14. Hudoklin Alenka, Stadler Alenka: Varno elektronsko trgovanje s pomočjo kreditnih kartic. Organizacija, Kranj, 30 (1997), 5, str. 288-289.
15. Iglič Damjana: Upravljanje s tveganji kartičnega poslovanja v bankah. Prikazi in analize VI/3, Ljubljana, 1998, 3, str. 54-58.
16. I. M. S.: Za varno uporabo kartic. Bančnik, Ljubljana, 1998, 5, str. 13.
17. Ivanovič Žarko: Preprečevanje zlorab v luči nove zakonodaje. Bančni vestnik, Ljubljana, (4) 1995, 4, str. 41-44.
18. Janjoš Željko: Ček. Bančnik, Ljubljana, 1998, 7, str. 18-19.

19. Kalakota Ravi, Whinston B. Andrew: Electronic commerce: a manager's guide. Reading: Addison-Wesley, 1997. 431 str.
20. Klapš Srečko: Ponudba plačilno-kreditnih in bonitetnih kartic v Sloveniji. Kapital, Maribor, 5 (1995), 98, str. 22-28.
21. Klapš Srečko: E-bančništvo na pohodu ... Kapital, Maribor, 9 (1999), 207, str. 22-29.
22. Koruza Dušan: Elektronsko bančništvo - trend sodobnega bančništva. Bančnik, Ljubljana, 1995, 4, str. 3-5.
23. Logar Miha: Denar in pamet na eni kartici. Bančni vestnik, Ljubljana (44) 1995, str. 29.
24. Logar Miha: Troboj plastičnih kartic. Bančni vestnik, Ljubljana, (45) 1996,1-2, str. 37.
25. McKeown G. Patrick: Information tehnology and the Networked Economy. Forth Worth: Harcourt College Publishers, 2001. 395 str.
26. Mesarič Jure: Ni bojazni za plačilne kartice. I&T, Ljubljana, 1 (2001), 10, str. 12-13.
27. Mušič Matjaž: Pametne kartice osvajajo elektronsko bančništvo. Bančnik, Ljubljana, 2000, april, str. 19.
28. Miš Svoljšak Irena: Telefonsko bančništvo: Halo, je tam banka?. Kapital, Maribor, 7 (1997), 168, str. 24-25.
29. Miš Svoljšak Irena: Elektronsko bančništvo: V tujini se elektronsko bančništvo še povečuje. Kapital, Maribor, 9 (1999), 207, str. 30.
30. Novak Karmen: Sodobni plačilni instrumenti. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 1996. 57 str.
31. Pepelnjak Ivan, Bradeško Marjan: Varnost računalniških sistemov in elektronskih transakcij. Zbornik: Banke in tveganja. Portorož: Zveza ekonomistov Slovenije, 1997, str. 161-164.
32. Pinterič Mojca: Smart Cards superseding cash. Slovenian Business Report, Ljubljana, 1995, 2, str. 19-21.
33. Sovka Peter: E-poslovanje: Osebna varnost. Kapital, Maribor, (11) 2001, 266, str. 49.
34. Šrajlehner Mirjana: Bankomate delajo na Škotskem. Kapital, Maribor, 11 (2001), 263, str. 26.
35. Šteblaj Alenka: Uporaba sodobnih plačilnih instrumetov v Sloveniji v letu 1998. Prikazi in analize VII/1, Ljubljana, 1999, 1, str. 61-80.
36. Šteblaj Alenka: Uporaba sodobnih plačilnih instrumetov v Sloveniji v letu 1999. Prikazi in analize VIII/1, Ljubljana, 2000, 1, str. 44-62.
37. Tomassini Irena: Na vogalu stoji bankomat. Mozaik, Ljubljana, 1999, 5-6, str. 40-41

38. Toplišek Janez: Elektronsko poslovanje. Ljubljana: Založba Atlantis, 1998. 336 str.
39. Trampuž Mitja, Cajhen Janko: Elektronsko bančništvo - novi izzivi. Zbornik: Banke in tveganja. Portorož: Zveza ekonomistov Slovenije, 1999, str. 160-161.
40. Žiberna Jožko, Ivanjko Šime: Menica in ček. Ljubljana: Gospodarski vestnik, 1993. 324 str.
41. Žnuderl Branko: Banke v očeh komitentov. Kapital, Maribor, 11(2001), 274, str. 26-27.

VIRI

1. Biometrics and the Future of Banking.
[URL: http://www.bankinfo/security/biometrics.html].
2. Credit Card and Check Fraud.
[URL: http://www.bankinfo/security/screditcard.html].
3. CERT/CC Statistics 1988-2001.
[URL: http://www.cert.org/stats/cert_stats.html].
4. Digitalna potrdila javnih ključev in overitelji.
[URL: http://www.gov.si/tečaj/kripto/kr-cert.htm].
5. Digitalen podpis.
[URL: http://www.gov.si/tečaj/kripto/kr-podp.htm].
6. WTLS (Wireless Transport Layer Security).
[URL: http://www.gov.si/tečaj/kripto/wtls.htm].
7. Sodobni plačilni instrumenti.
[URL: http://www.bsi.si/html/publikacije/bilteni/bil2001_12pdf].