

UNIVERZITET SINGIDUNUM
MASTER AKADEMSKE STUDIJE

STUDIJSKI PROGRAM:

SAVREMENE INFORMACIONE TEHNOLOGIJE -
ZAŠTITA INFORMACIONIH SISTEMA I DIGITALNA FORENZIKA

NASTAVNI PREDMET:

ELEKTRONSKO POSLOVANJE

Softverski proizvod
"Cash Teleport"
za bezbedne transakcije putem mobilnog telefona

- Master rad -

Mentor:
Prof. dr Milan Milosavljević

Student:
Đorđe Medaković
Br. indeksa:410318/2011

Beograd, 2012

SADRŽAJ

I	UVOD	3
II	ELEKTRONSKO BANKARSTVO	7
1.	Elektronsko bankarstvo. Pojam i definicija	9
2.	Elektronski sistemi plaćanja	10
2.1.	Plantne kartice	10
2.2.	Sistemi plaćanja bazirani na elektronskom novcu	17
2.3.	Digitalni ček	25
2.4.	Mikro plaćanja	27
2.5.	S.W.I.F.T.	28
2.6.	Sistemi EFT/POS	29
2.7.	Sistem ATM-ova	31
3	Tipovi elektronskog bankarstva	33
3.1.	Kućno bankarstvo (Homebanking)	33
3.2.	On-line bankarstvo	35
3.3.	Internet bankarstvo	36
3.4.	Mobilno bankarstvo	43
4.	Identifikacija i analiza rizika u e-bankarstvu	46
5.	Istraživanje trenda razvoja mobilnih plaćanja	47
6.	Obezbeđivanje sigurnosti transakcija na internetu	48
III	SOFTVERSKI PROIZVOD „CHASH TELEPORT“	58
1.	Šta je softverski proizvod „Chash Teleport“	58
2.	Način rada	60
3.	Tehnička implementacija	61
4.	Prednosti softverskog proizvoda „Chash Teleport“	61
5.	Potencijalni korisnici	62
6.	Kriterijumi bezbednosti	62
IV	EVALUACIJA KRIPTOGRAFSKE SIGURNOSTI SOFTVERSKOG PROIZVODA „CHASH TELEPORT“	63
1.	Polazišta evaluacije kriptografske sigurnosti „Cash Teleport“	63
2.	Opšta paradigma zaštite poruka	63
3.	Kriptografski ključevi	64
4.	Kriptografsko procesiranje na klijentskoj strani	64
5.	Kriptografsko procesiranje na serverskoj strani	65
6.	Kriptografsko procesiranje A	66
7.	Kriptografsko procesiranje B	67
8.	Zaključna diskusija kriptografske evaluacije	70
V	ZAKLJUČAK	71
VI	LITERATURA	73

I UVOD

Moderno bankarsko poslovanje suočava se sa sve većim izazovima, prvenstveno zbog napredka informaciono komunikacionih tehnologija. Nakon uspešnog uvođenja e-poslovanja, pred bankama se pojavio novi izazov – mobilna trgovina **m-commerce**.

U ovom radu predstavljene su mogućnosti, rizici i koristi koje mogu nastati, kao i jedno autorsko rešenje koje bankama nudi kao izlaz na mobilno tržište, u cilju ostvarivanja maksimalne vrednosti i satisfakcije korisnika usluga banaka.

Akcent rada je na rešavanju identifikovanih najvažnijih nedostataka m-commerce aplikacija, kao što su pitanja autentifikacije, sigurnosti i privatnosti mobilnih telekomunikacionih mreža.

Softverski paket "Cash Teleport" je nastao kao rezultat iskustva stečenog u dugogodišnjem radu u kompaniji "Telenor", kao jednoj od vodećih telekomunikacionih mobilnih operatera, kao i znanjima stečenim na specijalističkim studijama iz domena bezbednosti informacionih sistema i elektronskog poslovanja, Fakulteta za poslovnu informatiku, SINGIDUNUM, u Beogradu.

Softverski paket "Cash Teleport" se zasniva na konceptu ujedinjenja funkcija mobilnog telefona i platne kartice, koji je kao inovativno rešenje patentirano i uneto u evidenciju i deponovanje autorskih dela i srodnih prava Zavoda za intelektualnu svojinu. U želji da se ovaj inovativni koncept stavi u primenu, kreirana je poslovna aplikacija bezbedne transakcije novca putem mobilnog telefona "Cash Teleport" koja je takođe patentirana i uneta u evidenciju i deponovanje autorskih dela i srodnih prava Zavoda za intelektualnu svojinu u Beogradu.

Master rad predstavlja aplikativno rešenje bezbedne transakcije novca putem mobilnog telefona „**Cash Teleport**“, kao jedan od najvažnijih, ako ne i najvažnijem, zahtevu mobilnog bankarstva.

U I delu rada obrađeni su aspekti elektronskog bankarstva i sublimirani sistemi i tipovi elektronskog bankarstva, identifikovani rizici i trendovi daljeg razvoja. Poseban akcent stavljen je na obezbeđivanje sigurnosti transakcija na internetu.

I II delu rada opisan je softverski paket "Cash Teleport", način rada, tehnička implementacija, prednosti korišćenja i t.d.

III deo master rada obuhvata evaluaciju kriptografske sigurnosti softverskog proizvoda "Cash Teleport", koju je izvršio Matematički institut SANU.

IV deo praktični prikaz šifrovane SMS komunikacije.

ЗАВОДУ ЗА ИНТЕЛЕКТУАЛНУ СВОЈИНУ
Београд, Змај Јовина 21

Образац: А-1

**ПРИЈАВА ЗА УНОШЕЊЕ У ЕВИДЕНЦИЈУ И ДЕПОНОВАЊЕ
АУТОРСКИХ ДЕЛА И ПРЕДМЕТА СРОДНИХ ПРАВА**

1) Подносилац пријаве - носилац(и) ауторског права:
Borđe Medaković, Beograd, Makenziјеva 17 JMBG 0807979710098
Čedomir Vasić, Beograd, Kumodraška 334, JMBG 2607977710064
Dejan Živković, Beograd, Kumodraška 334 ili Mionica-Paštrić
JMBG 1411975771028

2) Пуномоћник:
Adv. Milovan Živković, Beograd, A. Glišića br. 4
АДВОКАТ
Милован М.Живковић
А.Глишића 4, Београд

3) Псеудоним или знак аутора:

4) Наслов ауторског дела:
Poslovna aplikacija bezbedne transakcije novca putem
mobilnog telefona "CASHTELEPORT"

5) Врста ауторског дела:
Poslovni aplikacioni paket

6) Форма записа ауторског дела:
Tekstualna forma i pilot aplikacija u PHP formatu

7) Подаци ако је у питању ауторско дело прераде:

8) Подаци о аутору, ако подносилац пријаве није аутор:

МИНИСТАРСТВО ЗА УНУТРАШЊЕ
ЕКОНОМСКЕ ОДНОСЕ
ЗАВОД ЗА ИНТЕЛЕКТУАЛНУ СВОЈИНУ
БЕОГРАД

ПРИЉЕПНО 14 JUL 2005

Орг. јед.	Врста	Позив	Бројност
12758/05 А		266	05

Слика 1: пријава ауторског дела Cash teleport



САВЕЗНА РЕПУБЛИКА ЈУГОСЛАВИЈА
САВЕЗНО МИНИСТАРСТВО ПРИВРЕДЕ
И УНУТРАШЊЕ ТРГОВИНЕ
Савезни завод за интелектуалну својину

Број: А-40/02/2
Датум: 30.09. 2002. године
Београд

ЈР

На основу члана 170. Закона о ауторском и сродним правима ("Службени лист СРЈ" бр.24/98), Савезни завод за интелектуалну својину издаје

ПОТВРДУ
О УНОШЕЊУ У ЕВИДЕНЦИЈУ И ДЕПОНОВАЊУ
АУТОРСКИХ ДЕЛА И ПРЕДМЕТА СРОДНИХ ПРАВА

Подносиоцу пријаве број А-40/02 од 05.04.2002.године, за уношење у евиденцију и депоновање ауторских дела и предмета сродних права, чији је подносилац Медаковић Ђорђе, Београд, ул. Макензијева бр.17., потврђује се да је

дело под насловом: Концепт уједињења функција мобилног телефона и кредитне картице

врста дела: писано дело,чланак (штампани текст)

на коме је као **аутор** назначен подносилац пријаве Медаковић Ђорђе, Београд, ул. Макензијева бр.17.,депоновано и унето у евиденцију депонованих ауторских дела и предмета сродних права у Савезном заводу за интелектуалну својину, дана 05.04.2002.године, под редним бројем **296**.

Достављено:

- Подносиоцу пријаве
Медаковић Ђорђе
Београд, ул. Макензијева 17
- Групи за ауторско и сродна права



Директор
Благован Карковић

Благован Карковић

Слика 2: пријава ауторског дела Концепт безбедне трансакције

МАТЕМАТИЧКИ ИНСТИТУТ САНУ
Кнеза Михаила 35
11001 Београд, п.ф. 367
Србија



MATHEMATICAL
INSTITUTE SANU
Kneza Mihaila 35
11001 Belgrade, P.O.B. 367
Serbia

Tel. 381-11-630170,
381-11-180591 (Library)
МАТЕМАТИЧКИ ИНСТИТУТ САНУ

Fax: +381-11-186105
e-mail: mi@mi.sanu.ac.yu

Бр. 42/1
31.01. 2007 год.
11000 БЕОГРАД, Кнеза Михаила 35
Поштомб. ф.п. 367

Saglasno Ugovoru br. 162/2 od 06. 10. 2006. godine između Grupe Autora koju zastupa Čedomir Vasić, Beograd (u daljem tekstu Naručilac) i Matematičkog instituta SANU, Beograd (u daljem tekstu MI-SANU) daje se sledeća

IZJAVA

o evaluaciji kriptografske sigurnosti CashTeleport kriptografskog metoda (u daljem tekstu: CashTeleport)

- MI-SANU je realizovao evaluaciju kriptografske sigurnosti CashTeleport-a od 15.11.2006. godine do 20.12.2006. godine. Rezultati evaluacije su sumirani u odgovarajućem tehničkom izveštaju (u daljem tekstu Izveštaj-DeoI) koji je dostavljen Naručiocu. Evaluacija je vršena na osnovu dostavljenog tehničkog opisa koje je dat u prilogu Izveštaja-DeoI. Saglasno stavovima iznetim u Izveštaj-DeoI konstatovano je da inicijalna verzija CashTeleport-a nema odgovarajuću kriptografsku sigurnost i da je potreban re-dizajn.
- Redizajn CashTeleport-a je realizovan u MI-SANU od 20.12.2006. godine do 25.01.2007. godine u saglasnosti sa stavovima Naručioca. Redizajniran CashTeleport prikazan u odgovarajućem tehničkom izveštaju (u daljem tekstu Izveštaj-DeoII) koji je dostavljen Naručiocu (u formi združenog Izveštaja koji obuhvata Izveštaj-DeoI i Izveštaj-DeoII).
- Redizajnirano CashTeleport kriptografsko rešenje obuhvata familiju partikularnih varijanti za kontrolu autentičnosti i zaštitu tajnosti podataka (videti Izveštaj-DeoII) koja pruža potencijal za ostvarivanje adekvatnog nivoa kriptografske sigurnosti. Nivo kriptografske sigurnosti partikularnih varijanti suštinski zavisi od selektovanih komponenti i setovanja parametara redizajniranog CashTeleport kriptografskog rešenja. Dati evaluacioni stav važi za razmatrani metod, i ne uključuje implementacione implikacije.
- Stav o redizajniranom CashTeleport se zasniva na tekuće važećim evaluacionim znanjima i zbog njihove vremenske promenljivosti treba da bude predmet povremenih re-evaluacija: Prva re-evaluacija treba da se realizuje po potrebi, a najkasnije za dve godine.

Beograd,
27. januar 2007. godine

Direktor Instituta
Dr Zoran Marković



Slika 3: Potvrda MI SANU

II ELEKTRONSKO BANKARSTVO

Elektronsko bankarstvo se danas podrazumeva u ponudi svake moderne banke. Dostupnost različitih, prilagodljivih i cenovno konkurentnih bankovnih usluga uz upotrebu modernih tehnologija, postaje temelj današnjeg bankarstva i društva. Elektronsko bankarstvo predstavlja pokušaj spajanja više različitih tehnologija, od kojih se svaka razvijala u drugom smeru i na drugačiji način: elektronski novac, platne kartice, ATM (bankomati), POS terminali, kućno bankarstvo, mobilno bankarstvo.

Prvi elektronski transfer novca izvršen je još davne 1860. godine. Transfer je izvršila firma *Western Union* iz SAD-a, uz pomoć telegrafa. Kasnije je telegrafski transfer novca postao uobičajen. Jedan od najvećih platnih i obračunskih sistema današnjice, američki *Fedvajer (Fedwire)*, započeo je sa radom 1918. godine, kao servis za telegrafski transfer novca pri Sistemu federalnih rezervi SAD-a.

Sredinom šezdesetih godina dvadesetog veka u Velikoj Britaniji i Sjedinjenim Državama broj transakcija u bankarstvu narastao je do neslučenih razmera. Primena tradicionalnih metoda obrade transakcija, jednostavno, više nije bila moguća, a problem je narastao do te mere da je pretio ugrožavanjem stabilnosti čitavog finansijskog sistema. Vlade Velike Britanije i Sjedinjenih Država su, krajem šezdesetih godina, preduzele mere za automatizaciju sitnijih transakcija u bankarstvu, pogotovo onih koje su repetitivnog karaktera. Na bazi ideje, do koje su vodeće britanske banke došle nekoliko godina ranije, u Sjedinjenim Državama je 1968. godine formirana radna grupa za unapređenje razmene „bez papira— (SCOPE — Special Committee on Paperless Entries), koja je funkcionisala pri Banci federalnih rezervi u San Francisku. Želja je bila da se stvori jeftin, pouzdan elektronski platni sistem, kao alternativa čekovima. Plan je bio jednostavan: pretvaranje periodičnih sitnih plaćanja čekovima (kao što su zarade i premije osiguranja) u posebno oblikovanu platnu evidenciju koja će moći da se „čita— uz pomoć računara. Rezultat ovih napora bila je prva *automatska klirinška banka* (ACH — Automated Clearing House), koja je počela sa radom 1972. godine.

Kao reakcija na povećanu tražnju za međunarodnim obračunom transakcija valutama i vrednosnim papirima, razvijeni su elektronski platni sistemi za plaćanja na veliko. U oblasti međubankarskog izveštavanja trenutno dominira *SWIFT*, koji je osnovan 1973. godine u Briselu. SWIFT je u vlasništvu njegovih članica, tj. konzorcijuma koji se sastoji od preko 2200 banaka.

Automatizacija transakcija u bankarstvu na malo dugo je odlagana zbog toga što je vrednost prosečne transakcije relativno mala. Pre samo desetak

godina cene neophodne opreme i infrastrukture za formiranje platnih sistema na malo bile su toliko visoke da bi troškovi za obradu jedne transakcije u novoformiranim sistemima bili veći od vrednosti same transakcije. Razvoj informacione i komunikacione tehnike i tehnologije, međutim, već danas omogućava automatizaciju transakcija u bankarstvu na malo uz prihvatljive troškove po jednoj transakciji. Za tehnologizaciju bankarstva na malo, dakle, od ključnog su značaja trendovi u informacionoj i komunikacionoj tehnologiji: upotreba javnih računarskih mreža (pre svega Interneta), kao i razvoj i primena metoda kriptografije. Trendovi u informacionoj i komunikacionoj tehnologiji, kao što je smanjenje troškova računarske obrade podataka, razvoj digitalne bežične komunikacije, standardizacija i sl., utiču na smanjenje cena računarske i komunikacione opreme, čime se smanjuju troškovi po jednoj transakciji u bankarstvu na malo.

Nova revolucija u oblasti tehnologizacije bankarstva na malo, međutim, bazirana je na ideji da se za automatizaciju transakcija u bankarstvu na malo ne formira nova infrastruktura, već da se iskoristi postojeća infrastruktura javnih računarskih mreža, pre svega Interneta. Internet spada u javne, tj. otvorene mreže, kojima svako ima neograničen pristup. Upotreba Interneta za automatizaciju transakcija plaćanja na malo povoljna je zbog niskih troškova po jednoj transakciji. Veliki problem, međutim, predstavlja nedovoljna bezbednost transakcija koje se obavljaju preko Interneta. Zbog toga korišćenje kriptografije predstavlja veoma važnu sigurnosnu meru prilikom dizajniranja platnih sistema i protokola.

Elektronske transakcije mogu se podeliti na analogne i digitalne. Transfer novca putem telegrafa je elektronska transakcija, ali elektronska transakcija analognog tipa. Digitalne elektronske transakcije vezane su, međutim, za pojavu elektronskih digitalnih računara. Primena savremenih elektronskih digitalnih računara u oblasti bankarstva omogućila je pojavu elektronskih transakcija digitalnog tipa. Razvoj elektronskog bankarstva u današnjem smislu reči započeo je krajem šezdesetih i početkom sedamdesetih godina dvadesetog veka.

Uporedo sa razvojem informaciono-komunikacionih tehnologije, dešava se evolucija bankarskog poslovanja, koja se odvijala u nekoliko faza.

- U prvoj fazi, **fazi inicijative**, informaciono-komunikaciona tehnologija se počinje shvatati kao osnova za sticanje konkurentne prednosti.
- Druga razvojna faza, **faza interaktivnosti**, dovodi do promene shvatanja filozofije pružanja bankarski usluga. Off-line bankarske usluge počinju ustupati mesto on-line uslugama, što znači da klijenti sve manje

odlaze u banku, jer im banke nastoje pružiti usluge u njihovim kancelarijama ili kućama.

- U trećoj razvojnoj fazi, **fazi personalizacije**, on-line usluge su dominantan oblik poslovanja između banke i komitenata.
- Četvrta faza, **faza virtuelizacije**, nastaje uporedo sa razvojem Interneta i stvaranjem virtuelnih banaka, banaka koje ne postoje fizički već kao web sajt kojem se klijenti obraćaju.

1. Elektronsko bankarstvo. Pojam i definicija.

Elektronsko bankarstvo je proces koji dozvoljava klijentima da obavljaju poslove elektronskim putem. Elektronsko bankarstvo može se realizovati putem Interneta ili posredstvom drugih specijalizovanih kompjuterskih mreža koje čak ne moraju biti bazirane na Internet tehnologijama, ako klijent ima otvoren račun sa njegovim informacijama koje su zaštićene lozinkom.

E-bankarstvo se neko vreme pojavljivalo u formi automatskih mašina-blagajnika i transakcija putem telefona. Nedavno, transformisao ga je Internet, novi dostavni kanal za bankarske usluge koji koriste i banke i korisnici. Pristup je brz, pogodan, uvek dostupan, gde god se korisnik nalazio. Dodatno, banke mogu da obezbede efikasnije usluge i znatno smanje troškove. Na primer, tipična transakcija košta oko 1\$ u tradicionalnim „brick and mortar”—bankovnim filijalama, 0.60\$ putem telefonskog poziva, a 0.02\$ ako se obavi on-line.

E-bankarstvo takođe olakšava poređenje bankarskih usluga i proizvoda što povećava konkurentnost između banaka, podstičući banke da prodiru na nova tržišta šireći svoj geografski doseg (domašaj). Neki čak vide elektronsko bankarstvo kao priliku da zemlje sa nerazvijenim finansijskim sistemima preskoče razvojne etape. Korisnici u takvim zemljama mogu lakše koristiti usluge inostranih banaka i kroz bežičani komunikacioni sistem, koji se razvija mnogo brže nego tradicionalna „žičana”—komunikaciona mreža.

Istovremeno, e-bankarstvo je osetljivo na rizike - naročito upravljanje, zakonitost, operativnost, i ugled – koji su inherentni u tradicionalnom bankarstvu. To postavlja nove izazove. U odgovoru, mnogi nacionalni regulatori su već modifikovali svoje propise da bi postigli svoje glavne ciljeve: obezbediti sigurnost i čvrstoću domaćeg bankarskog sistema, unaprediti tržišne discipline, i zaštititi prava korisnika i javno poverenje u bankarski sistem.

2. Elektronski sistemi plaćanja

Završni čin svakog posla predstavljaju finansijske transakcije. Iako plaćanje i naplata nisu samo tehnička pitanja, tehnologija može značajno unaprediti obavljanje finansijskih transakcija, omogućavajući da se ona obave brže, tačnije, pouzdanije i komfornije. U savremenim uslovima poslovanja, kada tradicionalni načini plaćanja sve više gube na značaju, elektronski načini plaćanja u delikatnim internet transakcijama pokazuju se najkritičnijim segmentom svakog posla. Kao najčešće korišćena sredstva za obavljanje finansijskih transakcija u elektronskom poslovanju izdvajaju se:

- Platne kartice
- Pametne kartice (Smart Card) i elektronski novčanici (Electronic Wallet)
- Elektronski ili digitalni novac (Electronic Money, Digital Cash)
- Sistemi mikro plaćanja (Micropayment)

2.1 Platne kartice

Platna kartica je instrument bezgotovinskog načina plaćanja i instrument za podizanje gotovog novca kod izdavaoca kartice ili preko bankomata. To je mali komad plastike koji sadrži neko sredstvo za identifikaciju (potpis ili sliku), što omogućava osobi na koju kartica glasi da je koristi za navedene namene.

Neki od osnovnih termina u vezi sa platnim karticama su:

- **Poslovna banka** – Banka koja ima poslovni odnos sa nekim trgovcem i koja prima sve transakcije kreditnim/debitnim karticama od tog trgovca. Za poslovne banke (acquiring banks) se, takođe, koristi i termin trgovačke banke (merchant banks).
- **Autorizacija** - Čin odobrenja transakcije kreditnom/debitnom karticom nekom trgovcu od strane banke koja je izdala kreditnu/debitnu karticu
- **Autorizaciona šifra** - Šifra koju dodeljuje banka koja izdaje kreditne/debitne kartice prilikom njihove prodaje, a koja pokazuje da je data transakcija autorizovana.
- **Bankarska kartica** - Kreditna/debitna kartica koju je izdala neka banka. Visa i MasterCard su bankarske kartice. American Express i Discover nisu.
- **Naknadno zaduženje** - Transakcija kreditnom/debitnom karticom koja se vraća nazad trgovcu koji je izvršio prodaju. Ovo se dešava kada vlasnik kreditne/debitne kartice ne odobri plaćanje računa tvrdeći da uopšte nije dobio proizvod ili je, na bilo koji način, nezadovoljan njime. Vlasnici kartica trebalo bi da pokušaju da problem reše sa trgovcem pre

nego što zatraže od emitenta kreditne/debitne kartice da odbije plaćanje računa.

- **Elektronsko „prevođenje“ podataka** - Unos i obrada računa elektronskim putem. U momentu kupovine kreditnom/debitnom karticom trgovac dobija autorizaciju prodaje, da bi nakon isteka radnog vremena on „preveo“ podatke sa računa u elektronski oblik i poslao podatke iz POS terminala na obradu. Trgovci koji nisu osposobljeni za elektronsku obradu računa, već tu obradu vrše ručno, na kraju radnog dana nose sve račune u svoju poslovnu banku.
- **Nezavisna prodajna organizacija** - Nezavisne prodajne organizacije igraju značajnu ulogu u svim poslovnim oblastima. U industriji kreditnih/debitnih kartica nezavisne prodajne organizacije predstavljaju treću stranu između trgovca i poslovne (trgovačke) banke. Mnoga preduzeća nisu u mogućnosti da steknu status trgovca preko neke poslovne banke zbog toga što ih data banka smatra previše rizičnim, pa moraju da steknu status trgovca preko neke nezavisne prodajne organizacije.
- **‘Zamena’**- Transakcija koja se odvija između poslovne banke i banke koja emituje kreditne/debitne kartice.
- **Provizija za ‘zamenu’** - Provizija koju poslovna banka plaća baci koja emituje kreditne/debitne kartice radi obrade transakcija kreditnim/debitnim karticama koje se odnose na račun nekog vlasnika kartice. Ovu proviziju regulišu MasterCard i Visa, a ona se obično izražava u vidu procenta od ukupnog iznosa transakcije.
- **Trgovački diskont** - Procenat od maloprodajne cene koji trgovac plaća, u vidu provizije, poslovnoj banci za obradu transakcija kreditnim karticama. Ova provizija je obično veća od provizije za razmenu, koju poslovna banka plaća banci koja emituje kreditne/debitne kartice.
- **Trgovački status** - Neko preduzeće smatra se „trgovačkim“ onda kada ima ovlašćenje od strane neke poslovne banke, nezavisne prodajne organizacije ili druge finansijske institucije da prima kreditne kartice.
- **Račun** – Instrument koji pokazuje obavezu vlasnika kartice da plati izvesnu sumu novca emitentu kartice. To je papirni dokument koji vlasnik kartice potpisuje kada kupuje kreditnom karticom. Podaci sa računa mogu se „prevesti“ u elektronski oblik i poslati na obradu preko finansijskih mreža, a mogu se i lično dostaviti poslovnoj banci.

Uobičajena transakcija pomoću kreditne kartice odvija se na sledeći način:

- Trgovac izračunava vrednost kupljene robe i traži od kupca da plati.
- Kupac daje trgovcu kreditnu/debitnu karticu.
- Trgovac provlači kreditnu/debitnu karticu kroz POS terminal. Vrednost prodate robe se unosi ručno, ili se preuzima iz registar–kase.

- Trgovac podnosi podatke o kreditnoj/debitnoj kartici i vrednosti kupljene robe svojoj poslovnoj banci, sa zahtevom za autorizaciju. POS terminali su obično podešeni tako da zahtevaju autorizaciju u momentu prodaje, a stvarni prenos podataka sa računa vrši se kasnije.
- Poslovna banka zatim obrađuje transakciju, prosleđujući zahtev za autorizaciju banci koja emituje kreditnu/debitnu karticu. Broj kreditne/debitne kartice identifikuje vrstu kartice, banku koja ju je emitovala i račun vlasnika kartice.
- Ako vlasnik kartice ima dovoljno novca na svom računu da pokrije kupovinu (ili mu je odobrena kreditna linija), banka koja emituje kreditnu/debitnu karticu autorizuje transakciju i generiše autorizacionu šifru. Ova šifra se šalje nazad poslovnoj banci. Banka koja emituje karticu rezerviše novac na računu vlasnika kartice u iznosu koji je ekvivalentan vrednosti kupljene robe. Međutim, račun vlasnika kartice se još uvek ne zadužuje.
- Poslovna banka obrađuje transakciju, a zatim šalje šifru za odobrenje ili odbijanje POS terminalu trgovca. Svaki POS terminal ima svoj jedinstveni identifikacioni broj, tako da je institucija koja vrši obradu transakcija u mogućnosti da prosledi podatke upravo tom terminalu.
- Račun štampa POS terminal ili registar–kasa. Trgovac zahteva od kupca da potpiše račun, koji ga obavezuje da nadoknadi naznačeni iznos banci koja emituje kreditnu/debitnu karticu.
- Kasnije, u najvećem broju slučajeva uveče, kada se radnja zatvara, trgovac upoređuje autorizacije koje su memorisane u POS terminalu sa potpisanim računima. Kada izvrši proveru podudarnosti svih autorizacija sa potpisanim računima, trgovac će prevesti, ili preneti podatke o svakoj autorizovanoj transakciji kreditnom/debitnom karticom poslovnoj banci na depozit. Isto tako, on može deponovati kod banke i realne, potpisane papirne račune.
- Poslovna banka, za svaki pojedini račun, vrši sa odgovarajućom bankom koja je emitovala karticu ono što se naziva zamenom. Banka koja je emitovala karticu odobrava poslovnoj banci iznos konkretnog računa, umanjjen za iznos provizije za zamenu.
- Poslovna banka zatim deponuje iznos svih računa koje je podneo konkretni trgovac na njegov račun, umanjujući ga za diskontnu proviziju.

Platne kartice mogu se podeliti u tri grupe:

- kreditne kartice
- debitne kartice
- unapred plaćene kartice

Kreditne kartice sadrže određeni kreditni limit koji potrošač može koristiti prilikom kupovine robe ili povlačenja gotovine. To znači da je banka odobrila

vlasniku kreditne kartice unapred određenu kreditnu liniju. Plaćanje kreditnim karticama može se vršiti svima onima koji su sa izdavaocem tih kartica stupili u ugovorenu obavezu da će pri njihovom prezentiranju davati imaocima robu ili usluge. Pri tome je vlasnik kreditne kartice dužan uz prezentaciju kreditne kartice da potpiše račun koji prodavac robe ili davalac usluga dostavlja izdavaocu kreditne kartice od koga vrši naplatu u ugovorenom roku.

Klijent banke kome je banka izdala kreditnu karticu ima odvojen račun po kreditnoj kartici od njegovog tekućeg računa. On obično na mesečnoj osnovi dobija stanje na računu kartice. Izveštaj sadrži detaljne informacije o svakoj transakciji koja je načinjena karticom tokom obračunskog perioda na koji se izveštaj odnosi, uključujući i iznos eventualno obračunate kamate i drugih troškova. Pored toga, u izveštaju je posebno prikazan iznos koji treba da se uplati na račun kreditne kartice u cilju otplate iskorišćenog kredita kao i datum do kojeg uplatu treba izvršiti. Odobreni kredit, tj. dužnički saldo na tom računu može se u celosti isplatiti na kraju meseca ili se može isplaćivati u ratama, pri čemu neizmireni dug prelazi u produženi kredit na koji banka naplaćuje kamatu. Pored toga, neke banke naplaćuju i godišnju taksu ili članarinu od vlasnika kartice. Postoji i obrtno (revolving) kreditiranje. Klijent je na kraju obračunskog perioda dužan da plati samo određeni deo svog mesečnog zaduženja (obično je to 10-20 odsto ukupnog duga), a ostatak dugovanja se prenosi u sledeći obračunski period. Na taj preostali dug banka zaračunava fiksnu kamatu.

Debitna kartica omogućava vlasniku da direktno zaduži svoj račun kod banke. Vlasnik ove kartice posle kupovine nema period slobodnog kredita. To znači da komitent putem daljinskih komunikacionih veza povlači novac sa svog tekućeg računa kod banke, bez potrebe da fizički dođe u banku. Debitne kartice mogu se koristiti u trgovinskim radnjama koje su snabdevene POS terminalima ili bankarskim automatima (ATM).

S obzirom na činjenicu da se vlasnik debitne kartice, koji povlači novac ili vrši plaćanje za kupovinu roba ili usluga, odmah se zadužuje na svom računu kod banke, debitne kartice su povoljne za prodavce, odnosno davaoce usluga, na čiji račun se takođe trenutno transferišu sredstva. Međutim, vlasnik debitne kartice ima mogućnost korišćenja sredstva samo do iznosa pokrića na svom računu kod banke. Pod određenim uslovima, debitne kartice mogu poslužiti i kao kreditne, ali je za to potreban poseban ugovor između banke koja je izdala karticu i prodajnog mesta.

Unapred plaćene kartice sadrže kompjuterski čip na koji se "ubacuje" iznos novca sa računa vlasnika kartice ili gotovinskom naplatom od njega. Na ovim karticama je uskladištena određena vrednost, odnosno unapred uplaćena sredstva koja su na raspolaganju klijentu. Prilikom kupovine roba

ili korišćenja usluga taj iznos se smanjuje korišćenjem terminala na prodajnim mestima. Unapred plaćene kartice mogu biti jednonamenske i višenamenske. Jednonamenske kartice su obično jednokratne tako da se po iskorišćavanju na njima uskladištenih vrednosti ne mogu "dopuniti" i ponovo koristiti. Primer takvih kartica su kartice za telefonske govornice, za parking, mobilne telefone.... Za razliku od ovih, višenamenske kartice se mogu "puniti" i one se koriste kao opšte sredstvo plaćanja na mestima koja su snabdevena specijalnim terminalima.

Unapred plaćene kartice predstavljaju jedan od oblika elektronskog novca. Ali ovde spadaju samo višenamenske unapred plaćene kartice, zbog toga što elektronski novac poseduje dve osnovne karakteristike: unapred plaćena novčana vrednost od strane vlasnika elektronskog novca i široka prihvatljivost te elektronske vrednosti u plaćanjima za niz roba i usluga. Prema tome, unapred plaćene kartice kojima se vrši samo jednonamenska plaćanja ne spadaju u koncept elektronskog novca.

Da bi vlasnik elektronskog novca mogao da ga koristi za plaćanja, on mora prethodno da kupi određenu vrednost elektronskog novca u zamenu za konvencionalni novac. Kupovinom elektronskog novca on vrši "plaćanje unapred", jer unapred kupuje željeni iznos elektronskog novca koji će kasnije upotrebljavati za plaćanja, za razliku od debitnih kartica gde se vrši "plaćanje sada" i kreditnih kartica gde vlasnik vrši "plaćanje kasnije".

Kod platnih kartica sigurnost je obezbeđena putem personalnog identifikacionog broja koji se sastoji od digitalnih znakova i ugrađen je na magnetnu traku ili čip, u zavisnosti od vrste kartice. Po ovom kriterijumu, kartice se mogu podeliti na:

- kartice sa magnetnom trakom i
- pametne kartice (smart kartice).

Kartice sa magnetnom trakom

Današnja tipična kreditna kartica, pored utisnutih podataka o korisniku i izdavaču, sadrži i magnetni medijum nanešen u obliku trake na površinu kartice. Ovaj medijum, na koji se podaci zapisuju na sličan način kao na magnetnu audio traku, sadrži podatke vezane za korisnika kartice, poput ličnih podataka, broja računa ili PIN-a. Ti podaci se nanose u formatu koji je definisan međunarodno prihvaćenim standardom, a u zavisnosti od broja staze na traci, kojih na uobičajenoj magnetnoj traci ima tri. Međunarodna organizacija za standardizaciju ISO, donela je standarde koji se, s vremena na vreme, dopunjuju novim specifikacijama i usklađuju sa aktuelnim tehnološkim dostignućima i zahtevima korisnika. Standardima su definisane tačne dimenzije platnih kartica, položaj magnetne trake na kartici, kao i sadržaj staza 1, 2 i 3. Platne kartice najčešće koriste samo stazu 2. Podatke

sa magnetnog medija može pročitati uređaj pomoću kojeg se vrše transakcije.

Sam proces plaćanja karticama sa magnetnim zapisom može se predstaviti sledećom procedurom: korisnik stavi svoju karticu u uređaj pomoću kojeg vrši plaćanje i unosi svoj PIN. Unešeni PIN se upoređuje sa onim zapisanim na samoj kartici i omogućuje se transakcija ukoliko je korisnik ispravno identifikovan. Uređaj pročita broj korisnikovog računa i uspostavlja telefonsku vezu sa centralnim računarom koji sadrži podatke o računu. Tada se vrši željena transakcija.

Usavršene kartice sa magnetnom trakom mogu se produktivnije koristiti, jer se na bazi porasta gustine same magnetne trake, obezbeđuje veći kapacitet memorije. Međutim, unapređenje bitno povećava troškove kako kartice, tako i terminala za njihovo korišćenje. Činjenica da su kartice sa trakom u svetu već dugo u masovnoj upotrebi, govori da će se ova vrsta kartica još dugo zadržati. Nedostaci koje ove kartice imaju nisu mali. Troškovi telefonskih linija kojim terminali komuniciraju sa centralnim računarima su vrlo veliki, dok je broj transakcija koje se obave toliko mali, da gotovo ne pokrivaju niti troškove obrade na ovakav način.

Smart kartice

Plastične kartice sa mikro čipom, nazivaju se pametnim ili inteligentnim karticama (*smart card*, *intelligent card*). Ova kartica, koja po izgledu podseća na običnu kreditnu ili debitnu karticu, poseduje jedan detalj koji je odvajaju od njih, a to je integrisano kolo ili čip. Čip je, u suštini, mikroprocesor sa memorijskim kapacitetima u kojima se mogu pohraniti značajne količine informacija. Uz mogućnost memorisanja informacija, čip na pametnoj kartici takođe može obrađivati informacije, što znači da su u njemu ugrađeni programi. Zavisno od vrste ugrađenog čipa, pametne kartice mogu biti memorijske, procesorske ili kombinovane.

Smart kartica je ništa drugo nego PC u malom. To uključuje: procesor (CPU), pomoću koga se vrše izračunavanja; Read-Only Memory (ROM), memorija na kojoj se nalazi operativni sistem, Random Access Memory (RAM), memorija koja se koristi za privremeno skladištenje prilikom rada procesora i Electronically Erasable and Programmable Read-Only Memory (EEPROM), memorija u kojoj su smešteni podaci od interesa (broj tekućeg računa, sertifikati, ključevi i sl.). Zatim tu je Clock i ulazno izlazni sklop preko koga se komunicira sa okolinom (čitačem). Tipična smart kartica može imati 8-bit procesor koji radi na 5 MHz, 256 do 1024 B RAM-a, 6 do 24 KB ROM-a, 1 do 16 KB EEPROM-a.

Struktura koju poseduje Smart kartica omogućava uvođenje autonomnosti obrade podataka i porasta kapaciteta memorije. Zahvaljujući inteligenciji

kartice, moguće je razviti raznovrsne sigurnosne aplikacije u oblastima kao što su: zaštita pristupa računarima ili mreži, identifikacija, mobilna telefonija, elektronski novac, vozačka dozvola, zdravstveni karton, zaštita podataka, digitalni potpis, kuponi, zaštita autorskih prava, elektronska trgovina, itd.

Pošto smart kartica poseduje mikroprocesor, ima mogućnost da donosi odluke po određenim pravilima programiranim na čipu, bez potrebe da se kontaktira host izdavaoca kartice. Time se ne opterećuju komunikacione linije, manji su troškovi prema Telekomu, a i smanjuje se opterećenje hosta. Da li će se raditi online ili offline, zavisi kako od same aplikacije na kartici, tako i od aplikacije na terminalu. Podaci koji se nalaze na kartici nikada ne napuštaju njeno bezbedno okruženje, otporni su na sve napade na operativni sistem. PIN je, za razliku od kartice sa magnetnom trakom, smešten na samoj kartici, te se za njegovu proveru ne mora kontaktirati host izdavaoca kartice. Pošto se PIN uopšte ne šalje preko komunikacione linije, povećava se nivo sigurnosti.

Izdavalac može kontrolisati korišćenje smart kartice i nakon izdavanja na bilo kom terminalu. Na primer, ako je neki korisnik kartice vremenom izgubio određeni kredibilitet koji je posedovao na početku, prilikom prvog on-line pristupa kartice na hostu, izdavalac može poslati komandu za blokiranje određene funkcije ili cele kartice. Ovim je kontrola korišćenja kartice od strane izdavaoca znatno povećana u odnosu na stanje koje je bilo sa karticama sa magnetnom trakom, tako da sigurnost kartice predstavlja još jednu od njenih prednosti.

Zbog hardverskih karakteristika, moguće je koristiti jednu karticu za više funkcija. Praktično rešenje koje se u svetu koristi uključuje debitno/kreditnu smart karticu kojoj je pridodato jedna ili više *Loyalty* funkcija. To znači da se istoj platnoj kartici pored osnovne, dodaju i dodatne funkcije u vidu npr. skupljanja poena koje korisnik dobija kupovinom određenih proizvoda. Smart kartica sadrži čak 100 puta više memorijskog prostora od magnetne kartice, kao i procesor pomoću koga su omogućena razna izračunavanja direktno na kartici. Ceo proces (npr. kriptovanje) počinje, traje i završava se na samoj kartici i nikakvi podaci ne napuštaju karticu što sistem čini izolovanim od spoljašnjeg sveta. Sprečeno je kloniranje i zloupotreba podataka sa kartice, a mogućnosti primene su višestruke. Naravno, ona ima i neke nedostatke:

- Kriptografski algoritmi stari oko 15 godina, mada se u svetu razvijaju novi kriptografski mehanizmi,
- Osetljive na vlagu,
- Osetljive na temperaturu (ukoliko se izlože temperaturi oko 60 stepeni, kartice više nisu za upotrebu),
- Osetljive na mehanička oštećenja,

- Jako su skupe ukoliko se izrađuju u malim serijama, postaju ekonomične tek kod masovnije upotrebe,
- Ograničen vek trajanja.

2.2 Sistemi plaćanja bazirani na elektronskom novcu

Najveće tehnološko dostignuće u razvoju bankarstva je pojava elektronskog novca, a samim tim i elektronskog bankarstva. Novac je u savremenoj interpretaciji, informacija. Kroz njega se markira pravo nekog subjekta u odnosu na robu i usluge koje egzistiraju u jednom društvu.

Elektronski novac se definiše kao specifična monetarna informacija koja se putem elektronskih impulsa u realnom vremenu prenosi između transaktora koji obavljaju plaćanja.

Elektronski novac omogućava kupovinu roba ili usluga pomoću računara u okviru komercijalnih računarskih mreža (npr.Interneta) ili poslovnih bankarskih mreža (npr.SWIFT-a). Praktično, elektronski novac u svakodnevnim transakcijama zamenjuje gotovinu i čekove. S druge strane, poslovnim subjektima omogućava da mimo uobičajenih kanala direktno posluju putem računarskih mreža.

Elektronski novac predstavlja sistem koji omogućava nekoj osobi da plati usluge ili robu prenoseći brojeve sa jednog računa na drugi. Brojevi elektronskog novca su unikatni, kao i serijski brojevi na pravim papirnim novčanicama. Svaki elektronski novac emituje neka banka i on predstavlja određenu sumu stvarnog novca. Jedna od ključnih osobina je, kao i kod pravog novca, anonimna upotreba, tj. kada kupac pošalje neki iznos digitalnog novca trgovcu, ne postoji način da se dobiju informacije o kupcu. Ovo je jedna od ključnih razlika između sistema baziranog na elektronskom novcu i sistema baziranog na kreditnim karticama. Još jedna ključna razlika je što primalac elektronskog novca može ponovo da ga koristi.

Elektronski novac se može koristiti za on-lajn kupovinu. Potrošači koji su zainteresovani za kupovinu elektronskim novcem imaju poseban softver na svom računaru koji im omogućava da podižu novac sa svog računa u banci u svoj —novčanik na računaru. Prilikom kupovine, oni razmenjuju ovako podignuti novac sa nekim trgovcem u zamenu za proizvode i usluge za proizvode koje žele da kupe. Banka koja prima depozite u elektronskom novcu, zatim otkupljuje novac koji je trgovac dobio.

Elektronski novac može se efikasno koristiti za elektronsku trgovinu samo ako postoji infrastruktura visokog tehničkog nivoa. Velika brzina prenosa podataka je osnovni preduslov za istovremeni prenos informacija o proizvodima potencijalnim klijentima. Pristup mora biti jednostavan i

ekonomičan. Domaćinstva moraju biti opremljena personalnim računarima sa odgovarajućim softverom. Kada su ispunjeni ovi tehnički uslovi, na red dolazi rešavanje problema bezbednosti.

Velika prednost elektronskog novca nad običnim je u tome da je on informacija u računaru koja može da se programira. Ova razlika omogućava da elektronski novac postane pametni novac u obliku tzv. "pametnih kartica". Dominantan oblik elektronskog novca je elektronski transfer sredstava na tački prodaje (EFT/POS) pomoću instaliranih terminala u trgovačkoj i uslužnoj mreži. Drugi oblik korišćenja elektronskog novca moguć je preko bankomata (Automated Teller Machines — ATMs), koji omogućavaju podizanje gotovine, polaganje depozita, prenos na druge račune i plaćanje sa različitih računa. Takođe, sve je veće korišćenje personalnih računara u kućama korisnika, što je dovelo do pojave homebanking sistema (*softver za lične finansije*) koji omogućavaju raspolaganje finansijskim sredstvima iz kuće, bez odlaska u banku.

Novim instrumentima omogućava se prvo udaljen ulaz na račune, njihovo korišćenje u svim varijantama i podizanje gotovine, da bi posle unapređenja samih instrumenata došlo do stvaranja potpuno novih instrumenata i aranžmana plaćanja, elektronskog novca koji se javlja u formi neke vrste elektronskog novčanika ili mrežnog elektronskog novca koji se distribuira preko zatvorene ili otvorene mreže.

Aranžmani za funkcionisanje prve kategorije elektronskog novca se pojavljuju u dve varijante:

- u prvoj, plaćanja predstavljaju praktično samo privremenu novčanu transakciju koja se finalno zatvara prenosom sredstava između transakcionih depozita kod bankarskih institucija,
- dok u drugoj, elektronski novac cirkuliše između korisnika na gotovo isti način kao i gotov novac, što znači da se plaćanje elektronskim novcem može smatrati finalnim već u ovom trenutku.

Plaćanja mrežnim elektronskim novcem se vrše između računa putem softvera koji poseduju razni korisnici ovog sistema plaćanja.

Sam elektronski novac u formi —elektronskog novčanika— bazira se na prethodno izvršenim uplatama monetarnih vrednosti koje su registrovane na mikročipovima elektronskih kartica, a mogu biti upotrebljene za plaćanje roba i usluga. Postojeći tipovi ovog novca još uvek nisu zakonska sredstva plaćanja u onom smislu u kome je to gotov novac iza koga stoje centralna banka i država i koji primaju svi, već samo onaj krug učesnika koji je uključen u određeni aranžman plaćanja usled čega mogu nastajati značajni pravni i monetarni problemi.

Poslovna filozofija lokacijskog približavanja usluga korisnicima nametnula je i ubrzani razvoj elektronskog bankarstva i njegovu standardizaciju. Banke su primorane da učestvuju u razvoju novog elektronskog bankarstva da ne bi izgubile svoju poziciju na tržištu.

Obavljanje potpunog bankarskog poslovanja direktno iz kuće, bez fizičkog prisustva u banci, danas je uobičajena pojava u razvijenim zemljama sveta. Banke koriste različite načine da klijentima omoguće što efikasnije i bezbednije obavljanje bankarskih transakcija iz kuće. Brojni su nazivi koje banke koriste za obavljanje ovih bankarskih aktivnosti. Najčešće korišćeni nazivi su: bankarstvo iz kuće (Home Banking), direktno bankarstvo (Direct Banking), on-line bankarstvo (On-line Banking), Internet bankarstvo (Internet Banking) i sajber bankarstvo (Cyber Banking). Postavlja se pitanje da li su ovi nazivi samo sinonimi ili potpuno različiti pojmovi. Često se pravi greška pri izjednačavanju pojmova Internet bankarstva i on-line bankarstva. Oba pojma označavaju obavljanje bankarskih transakcija iz kuće. Asortiman bankarskih usluga im je gotovo identičan, kao i sistemi zaštite. Međutim, razlike među njima znatno su veće.

U oblasti elektronskog novca posebno interesantno je pokretanje modela elektronskog novca od strane Citicorp-a. 1995. godine, direktor odeljenja za nove tehnologije, Shlomo Rosen, razvio je i patentirao ambiciozni poduhvat pod isto tako ambicioznim nazivom `elektronski monetarni sistem` (Electronic Monetary System — EMS). Cilj je bio da se stvori jedan sveobuhvatan platni sistem koji će moći da obavlja transakcije na veliko i na malo, a koji će biti podržan od strane najvećih američkih banaka.

Digitalne "novčanice" sastoje se od izvesnog broja bitova. Prema tome, postoji mogućnost kopiranja ovih novčanica i njihovog puštanja u optičaj. Ovaj fenomen poznat je pod nazivom "problem dvostrukog trošenja". Prema tome, platni sistem mora da poseduje mehanizme za prepoznavanje i prevenciju ponovljenih plaćanja istim digitalnim novčanicama.

Sistemi zasnovani na digitalnim novčanicama imaju problem u vezi s nominalnom vrednošću. Da bi se platio izvestan iznos moraju postojati digitalne novčanice sa odgovarajućom vrednošću, ili sistem mora biti sposoban da "vrati kusur" u obliku novih novčanica. Alternativno rešenje je da sve novčanice imaju istu, najmanju moguću nominalnu vrednost (npr. jedan cent, pa čak i manje). U tom slučaju bilo bi potrebno da se u optičaju nalazi ogroman broj digitalnih novčanica, čiju autentičnost treba neprestano proveravati.

Veoma je bitno omogućiti konvertibilnost elektronskog novca u "pravi" novac uvek kada potrošač to želi. Poverenje u neku elektronsku valutu znači

da treba da postoji stabilan "devizni kurs" između elektronske i realne valute. Ako su ovi kursevi nestabilni, ukazaće se mogućnost profitiranja po osnovu arbitražnih transakcija što bi smanjilo poverenje u elektronski novac zbog fluktuacije njegove vrednosti.

Elektronski novac se skladišti na računarskim fiksnim diskovima ili na nekom drugom medijumu. U slučaju kvara na konkretnom medijumu moraju postojati mehanizmi za povratak na originalno stanje pre kvara.

Značaj elektronskog novca povećava se sa povećanjem značaja Internet trgovine. Predstavljanje realnog novca u elektronskom obliku nužno zahteva preslikavanje karakteristika realnog novca, kao što su anonimnost, autentičnost i mogućnost sitnih plaćanja. U zavisnosti od načina implementacije digitalnog novca, postoje različite kriptografske metode i organizacioni preduslovi za izbegavanje upotrebe falsifikovanog novca. Postoje dve različite vrste novca zasnovanog na digitalnim novčanicama:

- Upotrebom specifičnih kriptografskih metoda može se postići anonimnost digitalnog novca. U tom slučaju ni finansijska institucija, ni trgovac, ne mogu uspostaviti vezu između potrošača i novčanica koje je on koristio. Finansijska institucija zna kom potrošaču su novčanice prenete na početku.
- Novčanice sa mogućnošću identifikacije potrošača omogućavaju finansijskoj instituciji da identifikuje potrošača i da prati plaćanja u kojima je data novčanica bila korišćena.

Pored toga, proces plaćanja može biti on-line i off-line. Kada je u pitanju on-line plaćanje, autentičnost novčanica mora biti proverena odmah. To znači da se neka digitalna novčanica koristi samo jednom. Finansijska institucija mora da proveri autentičnost korišćenjem spiska svih novčanica koje su emitovane. U slučaju off-line plaćanja, digitalne novčanice se mogu koristiti više puta. U cilju izbegavanja dvostrukog trošenja neophodno je smestiti informacije o korisniku ili korisnicima na samu novčanicu kako bi se provera mogla obaviti kasnije. Anonimnost može biti garantovana, a finansijska institucija će koristiti ove informacije samo u slučaju otkrivanja dvostrukog trošenja.

Trenutno na Internetu postoji nekoliko sistema elektronskog novca zasnovanih na „digitalnim novčanicama“ (digitalni novac). Najpoznatiji on-line sistemi su E-Cash firme DigiCash; NetCash, sistem koji je razvijen na Univerzitetu južne Kalifornije. Najpoznatiji of-lajn sistemi su Mondex i VisaCash.

DigiCash je pionir na području elektroničkog novca. Njegov osnivač je poznati kriptograf David Chaum, čiji radovi su u samom temelju tehnologije

elektroničkog novca. Preduzeće je osnovano 1990, ali zbog lošeg poslovnog upravljanja i neuspešnih pregovora s investitorima (među kojima su bili Visa, Microsoft, Netscape, Citibank, ABN Amro i drugi), bankrotiralo je 1998, a 16 patenata je prodato eCash Technologies (koja je takođe u problemima, otpustila je nedavno 25 od 65 zaposlenih). Elektronski novac koji je stvorio DigiCash se zove eCash. To je off-line proces plaćanja, koji koristi slepi potpis za postizanje anonimnosti. E-Cash novčanice su u fiksnim iznosima, i nije moguće povratiti razliku. Ako nije moguće platiti tačan iznos raspoloživim novčanicama, mora se obaviti usitnjavanje u banci. DigiCash eCash je u potpunosti implementiran u softveru. Korišćenje eCash-a zahteva posebnu aplikaciju na računaru klijenta. Ova aplikacija omogućava podizanje e-gotovine, polaganje e-gotovine u banku i slanje e-gotovine. Valuta koja se koristi zove se eBuck, a jedan eBuck vredi jedan USD. Novac je 1995. godine pušten u eksperimentalni rad i izdato je ukupno jedan milion eBucks-a.

CyberCash je osnovan 1994. godine. Dve godine kasnije postali su javna kompanija i prilikom početne emisije deonica uspeali su skupiti zavidan kapital. Popularnost su izgradili na ponudi tehnologije za mikroplaćanja (micropayments). Ova tehnologija nikada nije šire komercijalno profunkcionisala, i preduzeće je na kraju prešlo na pružanje usluga on-line autorizacije kreditnih kartica. Međutim, posao im je stagnirao, i na kraju 2001. godine objavili stečaj. Nakon toga, kupila ih je VeriSign, koji se bave izdavanjem digitalnih sertifikata.

Na Internetu trenutno postoji nekoliko sistema elektronskog novca zasnovanih na „digitalnim novčanicama“ (digitalni novac). Najpoznatiji on-line sistemi su E-Cash firme DigiCash i NetCash, sistem koji je razvijen na Univerzitetu južne Kalifornije. Najpoznatiji off-line sistem je Mondex.

E-Cash

E-Cash je anonimni digitalni novac čija se ispravnost proverava on-line, od strane odgovarajuće finansijske institucije. E-Cash sistem razvila je firma DigiCash, a od 1995. godine nudi ga Mark Twain Bank iz Sent Luisa.

Potrošači povlače digitalni novac sa svog E-Cash računa upotrebom tzv. „slepe metode“ i skladište ga na fiksnom disku svog računara. „Slepa metoda“ funkcioniše na sledeći način: Klijent šalje digitalnu novčanicu, sa šifriranim serijskim brojem, finansijskoj instituciji. Finansijska institucija „overava“ novčanicu i šalje je nazad klijentu. Klijent zatim dešifruje serijski broj. Prema tome, serijski broj nije poznat finansijskoj instituciji, što garantuje anonimnost. Da bi se sprečila dvostruka potrošnja, finansijska institucija mora da evidentira serijske brojeve svih prispelih digitalnih novčanica.

Pri svakoj kupovini preko Interneta, potrošač daje digitalne novčanice trgovcu. Trgovac odmah prebacuje ove novčanice u svoju banku, kako bi proverio da li su ispravne. Trgovčeva banka registruje brojeve emitovanih digitalnih novčanica, bez mogućnosti identifikacije potrošača koji ih je utrošio. Konačno, ako je sve u redu, saldo na računu trgovca povećava se za dati iznos, a trgovac isporučuje proizvode/usluge.

Proces plaćanja upotrebom E-Cash-a:

- 1.) potrošač šalje novčanicu sa šifrovanim serijskim brojem finansijskoj instituciji
- 2.) finansijska institucija vraća overenu novčanicu
- 3.) potrošač dešifruje serijski broj i koristi novčanicu za plaćanje
- 4.) trgovac šalje novčanicu svojoj finansijskoj instituciji
- 5.) proveru i kliring
- 6.) trgovac dobija potvrdu, a saldo na njegovom računu se povećava

Digitalne novčanice mogu se koristiti samo jednom. E-Cash se može smatrati valutom za sebe. Finansijske institucije moraju da koriste specijalne račune. One će, takođe, garantovati konverziju u realni novac. Zbog toga će centralne banke imati poteškoće pri kontrolisanju novčane mase, jer finansijske institucije mogu kreirati dodatni novac i time povećati novčanu masu.

Bezbednost E-Cash-a postiže se upotrebom asimetričnog kriptografskog algoritma. Pristup računu može dodatno biti zaštićen upotrebom ličnih lozinki. Registrovanjem serijskih brojeva digitalnih novčanica sprečava se dvostruko trošenje. Troškovi provere autentičnosti digitalnih novčanica su relativno veliki, jer provera treba da se obavi on-line.

To znači da je pogodnost ovog sistema za mikro-plaćanja (plaćanja u veoma malim iznosima) pod znakom pitanja. Svaka osoba koja ima E-Cash račun može da prima E-Cash novčanice. „Slepa metoda“, o kojoj je bilo reči, garantuje anonimnost.

NetCash

NetCash metoda je razvijena na Univerzitetu južne Kalifornije (University of Southern California). Značajna karakteristika ovog projekta jeste upotreba već postojećih računovodstvenih sistema i procedura u finansijskim institucijama. Ovo će uticati na smanjivanje početnih investicija.

Nasuprot E-Cash-u, ova metoda zasnovana je na jednom decentralizovanom pristupu. Shodno tome, problemi u vezi sa velikim

brojem novčanica i učesnika mogu se rešiti mnogo lakše. Zbog toga je prihvaćena delimična anonimnost, a potrebna je i kooperacija svih finansijskih institucija koje učestvuju u sistemu.

Sistem se zasniva na nezavisno distribuiranim novčanim serverima. Novčani serveri predstavljaju lokacije na kojima se anonimni novac zamenjuje za „ne-anonimni” novac. Svaki novčani server poseduje jedan račun na računovodstvenom serveru.

Kliring obavlja novčani server. Neophodno je da se potvrdi integritet ovih servera i da novčani serveri mogu da primaju novčanice sa drugih novčanih servera. NetCash novčanice imaju nominalnu vrednost i serijski broj. Pored toga, na njima je zabeležena adresa emisionog servera i datum njihovog isteka.

Proces plaćanja upotrebom NetCash-a:

1. potrošač podiže digitalne novčanice da bi izvršio plaćanje
2. potrošač šalje digitalne novčanice trgovcu, šifrovane pomoću asimetričnog algoritma
3. trgovac podnosi ove novčanice i dobija nove, ili se dati iznos prebacuje na njegov račun. Trgovac zatim šalje potvrdu potrošaču
4. finansijska institucija obavlja kliring

Potrošač podiže NetCash novčanice sa nekog novčanog servera. Ove novčanice se šifriraju putem javnog ključa i šalju trgovcu. Anonimnost potrošača može se garantovati upotrebom novog ključa za svaku poruku. Trgovac odmah prebacuje novčanice, koje je primio, svom novčanom serveru. Od svog platnog servera on dobija nove novčanice, ili se odgovarajući iznos prebacuje na njegov račun. Konačni kliring obavlja novčani server.

Serijski brojevi svih novčanica koje nisu vraćene nazad i koje nisu istekle skladište se u novčanom serveru, kako bi se sprečilo dvostruko trošenje. To znači smanjenu anonimnost. Anonimnost se može povećati razmenom ovih novčanica na drugom serveru.

Bezbednost se postiže pomoću kriptografskih algoritama. Kao i u slučaju E-Cash-a, i ova metoda zahteva dosta komuniciranja. Međutim, upotreba ove metode za mikro-plaćanja trebalo bi da bude efikasnija. Svaka osoba može da prima NetCash novčanice, jer sistem omogućava slobodnu razmenu novčanica.

Mondex

Mondex sistem digitalnog novca razvija firma Mondex U.K., koja je nakon kupovine kontrolnog paketa akcija od strane MasterCard-a, postala deo kompanije MasterCard.

Za razliku od prethodna dva sistema, Mondex je prvobitno razvijan kao off-line sistem, koji se sada prilagođava Internetu. Mondex je, u celini, zasnovan na karticama sa mikročipom, a jedinstven je po tome što omogućava transfer s kartice na karticu. Kao što je to slučaj kod E-Cash sistema, i Mondex koristi sertifikate koji glase na donosioca - novac se smešta na korisnikovu karticu. Međutim, za razliku od E-Cash-a, Mondex novac se sme prenositi sa jedne kartice na drugu beskonačan broj puta, bez potrebe nekog centralizovanog kliringa ili verifikacije od strane neke banke. Prema tome, Mondex je od svih sistema digitalnog novca najpribližniji realnom novcu.

Ključna razlika između Mondex-a i realnog novca je mogućnost praćenja transakcija koju pruža Mondex. Mondex kartice evidentiraju svaku transakciju putem jedinstvenog identifikatora, koji se može koristiti za praćenje transakcija, ako je to potrebno.

Centralni momenat kod Mondex-a je i bezbednost, koja postoji u dva primarna aspekta sistema: hardveru na kartici i procesu prenosa vrednosti. Mondex garantuje bezbednost sistema zasnovanog na karticama sa mikročipom. Suština Mondex-ove hardverske bezbednosti je da digitalni novac ne može da egzistira nigde osim na Mondex kartici.

Nijedna druga kartica sa mikročipom ili hardverski uređaj koji se „predstavlja” kao Mondex kartica ne može da komunicira sa pravom Mondex karticom. Mondex kartica otkriva „lažne” kartice i odbija da izvrši transfer novca na njih. Sistem se zasniva na činjenici da je svaka kartica „overena” Mondex-ovim digitalnim potpisom.

Sam proces transfera je, takođe, krajnje bezbedan. Kada se obavlja transfer između potrošača i trgovca, na primer, dve kartice ne samo da međusobno proveravaju autentičnost, već se transfer obavlja u sekvencama, tako da novac ne može istovremeno da egzistira na dva mesta. Novac se oduzima sa potrošačeve kartice pre nego što se upisuje na trgovčevu karticu. Transfer ne može da funkcioniše ni na koji drugi način.

Zbog činjenice da je Mondex sistem zasnovan na karticama, jedan od najvećih problema je taj što je potrebno da potrošači poseduju čitače kartica. Ovo nije jednostavan zahtev, pa mnogi tvrde da je firma DigiCash

bila u pravu kada je formirala E-Cash sistem, kao sistem baziran isključivo na softveru.

Jedna od najznačajnijih barijera za Mondex sistem jeste ekonomske prirode - bankama još uvek nije jasno kako će profitirati na njemu. Prvo, emisione institucije ne profitiraju od emisije. Emisija Mondex novca podrazumeva njegovu prethodnu kupovinu od Mondex-a. Tek onda neka finansijska institucija može da emituje Mondex novac svojim klijentima. Kad je novac već na tržištu, data finansijska institucija verovatno neće zarađivati provizije za obradu transakcija, zbog toga što ovaj sistem ne zahteva nužno prisustvo banaka, sem ukoliko neki korisnik ne želi da položi depozit, povuče novac ili, jednostavno, zameni Mondex karticu za gotovinu.

Ipak, ako ovu ekonomsku barijeru ostavimo po strani, možemo zaključiti da je Mondex najbolje osmišljeni model digitalnog novca baziran na hardveru, posmatrano na duži rok.

2.3 Digitalni ček

Čekovi su platni mehanizam koji je spor za plaćanje a sam proces plaćanja čekovima je poprilično nefunkcionalan i zahteva korišćenje koverta i markice. Sistemi digitalnog plaćanja čekovima nude neka rešenja.

Oni veoma brzo osvajaju tržište, posebno u poređenju sa svim ostalim negotovinskim platnim mehanizmima. Ovu konstantaciju potvrđuju sledeći podaci: 65 milijardi čekova je ispisano 2000-te godine, a broj se uvećava za oko 1 milijardu godišnje, što je tri puta veća stopa rasta u odnosu na stopu rasta kreditnih kartica, kartica zaduženja i ostalih oblika elektronskog transfera sredstava. Međutim, troškovi obrade čekova su svuda u svetu između 0.75\$ i 3.00, banka državnih rezervi SAD procenjuje da proces obrade čekova košta američku ekonomiju 44 milijardi dolara godišnje.

Sistemima digitalnog plaćanja čekovima teži se proširenju funkcionalnosti postojećih čekovnih računa, kako bi se omogućilo da se ovi računi koriste kao platni mehanizam prilikom online kupovine. Ovi sistemi mogu se posmatrati kao proširenje postojeće infrastrukture banaka i čekova. Neki od jednostavnijih sistema se koriste za elektronsko plaćanje pojedincima i za postavljanje računa na sajtove, na kojima se aukcija vrši online.

Proces naplate se odvija na sledeći način:

- banka izdaje ček kupcu
- kupac upisuje u elektronički ček iznos i datum, potpisuje ga svojim digitalnim potpisom i predaje trgovcu. Prazni ček već je pre bio

potpisan digitalnim potpisom banke koja ga je izdala. Trgovac izdaje robu kupcu.

- trgovac upisuje na ček svoj broj računa i prosleđuje e-ček svojoj banci, potpisujući ga svojim digitalnim potpisom
- trgovčeva banka proverava potpis trgovca i potpis banke izdavaoca i prosleđuje ček banci izdavaocu na naplatu
- banka izdavalac proverava svoj digitalni potpis i digitalni potpis kupca na dospelom čeku, proverava stanje novca na računu i, ako je sve u redu, prebacuje novac s računa kupca na račun trgovca.

E-ček predstavlja rizik za trgovca pošto ne može da zna da li kupac ima na svom računu u banci dovoljno novca za pokriće čeka. Osim toga, kupac može da falsifikuje svoj digitalni potpis. Ako želi da bude siguran, trgovac mora da ima on-line vezu s bankom izdavaocem čeka, što bitno komplikuje i poskupljuje transakciju jer banaka može biti mnogo.

Sistemi digitalnog plaćanja čekovima imaju niz prednosti:

- ne zahtevaju da korisnik obelodanjuje informacije o svom računu drugim pojedincima, prilikom učestvovanja na online aukcijama
- ne zahtevaju da kupci neprestano šalju vrlo poverljive finansijske informacije putem Web-a
- jeftiniji su za prodavce od kreditnih kartica
- transakcije digitalnim čekovima su mnogo brže od transakcija baziranih na tradicionalnom, papirnom čeku

ECheck sistem zahteva da korisnik dobije od svoje tradicionalne banke hardverski baziranu "elektronsku čekovnu knjižicu". Vrlo je važno napomenuti da je "elektronska čekovna knjižica" spoljni, hardverski priključak za korisnikov PC. Hardver može biti PCMCIA kartica, standardna PC kartica ili specijalizovan čitač smart kartice. Elektronska čekovna knjižica sadrži korisnikov digitalni potpis u obliku privatnog ključa, kao i javni ključ banke koja ju je izdala. Korišćenjem softera, koji obezbeđuje elektronska čekovna knjižica, korisnik ispunjava elektronski ček i šalje ga prodavcu putem Interneta. Ova veza (kupac – Internet – prodavac) je šifrovana, a podatak koji se prenosi sadrži korisnikov digitalni potpis, javni ključ i digitalni potpis banke koja je ček izdala. Po prijemu elektronskog čeka, prodavac proverava autentičnost digitalnih potpisa pošiljaoca i banke koja je ček izdala, korišćenjem njihovih ključeva, i deponuje ček u svoju banku. Viši nivo potvrđivanja autentičnosti, je Banka federalnih rezervi, koja potvrđuje javni ključ banaka koje izdaju elektronske čekove. Elektronski čekovi mogu sadržati broj fakture, doznaku i druge informacije. ECheck sistem je interesantan jer je "elektronska čekovna knjižica" fizički uređaj. Izabran je fizički uređaj, jer se smatralo da je ova varijanta mnogo sigurnija od kreiranja računa putem Interneta. Uređaj je prenosiv i vrlo ga

je teško neautorizovano koristiti. Iako su ovaj sistem razvile Banka federalnih rezervi i komercijalne banke, sa namerom da se u potpunosti uklopi u postojeći sistem čekova, eCheck ipak zahteva velike investicije u novu infrastrukturu.

2.4. Mikro-plaćanja

Mikro-plaćanja su elektronska plaćanja male vrednosti (napici, telefon, prevoz, parking, za kopiranje, za kopiranje Internet sadržaja, lutrija, kocka ...), koje su specijalizovano dizajnirane za elektronsku trgovinu na Internetu, pre svega za kupovinu nematerijalnih dobara. Mikro-plaćanja su zamena za sitan novac sa karakteristikama da je jeftin (keš je skup za manipulaciju), elektronski je pokretljiv, lakši je za prebrojavanje, proveru i verifikovanje. To su transakcije vrednosti ispod 1\$. Tehnološke uštede se ogledaju u tome što se ne vrši verifikacija svake transakcije i koristi se simetrična enkripcija. Metodi rada se zasnivaju na unapred unetoj vrednosti i njihovom grupisanju koji iniciraju da su učesnici u plaćanjima anonimni i da se smanjuju fiksni troškovi. Najpoznatiji sistemi su *MiliCent*, *CyberCoin* i *NetBill*.

Karakteristika MiliCent-a je ta da kupac kupuje karticu koja je kao telefonska i da za vreme plaćanja razmenjuje deo novca sa brokerom i vrši plaćanja, dok prodavac sakuplja delove i razmenjuje za novac. Svako se može registrovati kao broker. MiliCent je nastao kao projekat razvijen od strane DEC korporacije (Digital Equipment Corporation) i on ne nudi anonimnost u plaćanjima.

NetBill je istraživački projekat koji je započet na Institutu za informacione tehnologije pri Carnegie Mellon univerzitetu u saradnji sa organizacijama Mellon Bank-om i Visa-om, a delom su ga finansirale i Nacionalna fondacija za nauku i Agencija za napredne istraživačke projekte. U ovom sistemu NetBill ima ulogu treće strane, koja vrši proveru autentičnosti, upravlja računima, vrši obradu transakcija, fakturisanje i informisanje klijenata i korisnika u mreži.

U suštini Cyber Cash sistem se zasniva na računovodstvenom transferu odgovarajućih iznosa. CyberCash vrši transfer novca sa potrošačevog privremenog računa na trgovčev privremeni račun koji su, posebno za tu namenu, kreirani u CyberCash banci u Virdžiniji.

Osim ovih navedenih, postoje i drugi projekti za mikroplaćanja.

2.5. S.W.I.F.T.

Bezgotovinski transfer novca se vrši preko Svetske organizacije za međubankarsku finansijsku telekomunikaciju (SWIFT). SWIFT je organizovan 1973. godine u Belgiji kao neprofitabilno akcionarsko društvo sa zadatkom da zameni transfer sredstava telefonskim ili telegrafskim putem. U početku u ovu instituciju je bilo uključeno 239 banaka iz 15 država. Mreža SWIFT ima dva ključna centra u Holandiji i Sjedinjenim Američkim Državama koji komuniciraju putem satelita, sa institucijama koja uključuje nekoliko hiljada finansijskih institucija iz preko 200 država. U državama članica postoje regionalni centri, a veza između članica se uspostavlja preko međunarodnih i nacionalnih mreža.

Osnovne karakteristike SWIFT sistema su :

- unificiranost jezika komunikacije;
- visoka sigurnost i garantovana tajnost;
- trenutni prenos poruka;
- minimalne mogućnosti nastanka grešaka;
- efikasna kontrola;
- povezanost sa bankama širom sveta;
- mogućnost efikasnog upravljanja sredstvima;
- automatska obrada podataka;
- smanjivanje troškova poslovanja.

Poslovi se obavljaju preko tzv. SWIFT poruka. SWIFT poruka je standardizovana, sadrži određeni format i određeni broj polja koji se klasifikuje u kategorije:

- Doznake i čekovi,
- Transferi finansijskih institucija,
- Devizna tržišta, tržišta novca i derivata,
- Naplata i gotovinski inkaso,
- Tržište hartija od vrednosti,
- Plemeniti materijali i investicione grupe,
- Dokumentarni akreditivi i garancije,
- Putnički čekovi,
- Gotovinski menadžment i korisnički status.

Iza SWIFT poruka stoje poslovi:

- transferi korisnika,
- transferi banaka,

- slanje poruka o postojanju pošiljki za korisnike,
- menjački poslovi,
- depoziti i zajmovi,
- mogućnost pozajmice sredstava,
- plaćanje kamata,
- potvrde o slanju.

SWIFT poruke obuhvataju: doznake, bankarske doznake, devizno tržište i kreditne odnose, inkaso poslove, hartije od vrednosti, akreditive, posebne ponude.

Sve vrste poruka su standardizovane i iza njih mogu stajati različiti finansijski poslovi i različiti subjekti kao što su: transferi korisnika, transferi banaka, slanje poruka o postojanju pošiljke za korisnike, menjački poslovi, depoziti i zajmovi sa fiksnim ratama, mogućnost pozajmice sredstava, plaćanje kamate, potvrde o stanju.

Tipovi poruka – 9 kategorija :

- doznake i čekovi;
- transferi finansijskih institucija;
- devizna tržišta, tržišta novca i derivata;
- naplata i trgovinski inkaso;
- tržište hartija od vrednosti;
- plemeniti metali i investicione grupe;
- dokumentarni akreditivi i garancije;
- putnički čekovi;
- gotovinski menadžment i korisnički status.

SWIFT ADRESA

Univerzalna metoda kojom se indetifikuju finansijske institucije naziva se SWIFT adresa ili BIC-kod SWIFT adresa se sastoji od osam do jedanaest srodnih znakova grupisanih u sledeće komponente:

- šifra banke
- šifra zemlje
- šifra lokacije
- oznaka terminala
- oznaka filijale

2.6. Sistemi EFT/POS

POS terminal (Point-of-Sale terminal, tj. terminal na prodajnom mestu) je elektronski uređaj koji očitava magnetnu traku platne kartice i informaciju

o njoj kao i o iznosu transakcije putem stalne telefonske ili ISDN veze prenosi banci. Na isti način banka POS terminalu šalje povratnu informaciju na osnovu koje se štampa račun. Taj račun je po pravilu u duplikatu, s tim što prvi primerak vlasnik kartice potpisuje i ostavlja, a drugi zadržava za ličnu evidenciju.

POS terminal se nalazi na prodajnom mestu i omogućava plaćanje robe ili usluge karticom. To je uređaj koji očitava podatke sa kartice i na osnovu tih podataka se vrši kontrola validnosti kartice, kontrola stanja na računu kartice i, po uspešno izvršenom plaćanju, prenos sredstava sa računa kartice na račun trgovca u iznosu izvršene kupovine.

Prednosti instaliranja POS terminala:

- povećanje prodaje roba i usluga – sa karticom kupci nisu ograničeni na iznos novca koji imaju u novčaniku.
- jednostavnost prihvatanja kartica i smanjenje troškova – terminal je povezan sa bankom tako da se autorizacija i naplata svih transakcija odvija automatski.

POS terminal se postavlja na prodajnom mestu trgovca nakon sklapanja ugovora o prihvatanju kartica. Neophodno je da prodajno mesto ispunjava sledeće tehničke uslove:

- izvor napajanja – slobodan strujni priključak
- analogna telefonska linija (isti tip linija se koristi za povezivanje FAX-a ili računara) na mestu gde će se instalirati terminal.



Slika 4: POS i POS touchscreen

Sistemi elektronskih plaćanja u maloprodaji (Electronic Funds Transfer System/Points of Sale – EFT/POS) spadaju u najdinamičnije aplikacije elektronskog prenosa sredstava. Konceptijski, oni pružaju najčistiji elektronski prenos sredstava koji je do danas realizovan iz razloga što je pomoću njih omogućeno apsolutno eliminisanje papirnih instrumenata iz celokupnog procesa platno prometne transakcije.

Suština njihovog funkcionisanja sastoji se u mogućnosti aktiviranja terminala u maloprodaji određenom plastičnom karticom, koja služi kao

sredstvo ulaza i identifikacije, i obavljanja trenutnog prenosa sredstava sa računa kupca na račun prodavca. Sam mehanizam funkcionisanja zasniva se na povezanosti terminala lociranih na određenim prodajnim ili uslužnim mestima sa računarskim centrima određenih finansijskih institucija.

U zavisnosti od finansijskih institucija koje su uključene u sistem mogu se razlikovati tri modela. Prvi model je najjednostavniji i on se može primenjivati samo u lokalnim relacijama zato što podrazumjeva uslove u kojima i kupac i prodavac imaju račune kod jedne te iste banke. Drugi model je nešto složeniji, u njega su uključene dve ili više banaka koje između sebe obavljaju operacije automatskog kliringa. Treći model je model mreže, funkcioniše koristeći switching i processing centre i pogodan je za primenu u nacionalnim i međunarodnim relacijama. Današnji sistemi plaćanja, u maloprodaji, pripadaju trećoj kategoriji, koji ne samo da prerastaju u internacionalne sisteme, već i između vodećih svetskih sistema dolazi do međusobnih kooperacija.

EFT/POS sistemi su off-line ili on-line. U slučaju off-line sistema nije moguće vršiti direktnu trenutnu autorizaciju svake pojedinačne transakcije, kao što je moguće kod sistema zasnovanih na on-line vezi.

2.7. Sistemi ATM –ova

Jedna od najzastupljenijih vrsta tehnologije elektronskog bankarstva su bankomati – ATM (Automated Teller Machines). Osnovni cilj uvođenja terminala za komunikaciju između banaka i komitenata bio je automatizovanje rutinskih i svakodnevnih bankarskih aktivnosti. Samouslužni šalteri (eng. Automated Teller Machine – ATM) omogućavaju korišćenje kompletnih šalterskih usluga:

- deponovanje i podizanje novca,
- izdavanje čekovnih knjižica,
- naručivanje i primanje izveštaja,
- deponovanje i unovčavanje dokumenata plaćanja,
- transfer sredstava sa jednog racuna na drugi, i
- korišćenje kredita određivanjem limita za prekoračenje.

Bankomati su prvi korak ka elektronskom bankarstvu, a predstavljaju i neku vrstu elektronskih filijala banaka. Prvi bankomat se vezuje za filijalu britanske "Barclays" banke 1967. godine.

Bankomat predstavlja terminal za unos podataka s dva ulazna i četiri izlazna uređaja. Kao i svaki drugi terminal, on mora da bude povezan sa centralnim računarom, bilo putem iznajmljene linije ili modema. Veza iznajmljenom linijom je pogodnija za lokacije na kojima se obavlja veliki

broj transakcija, a modemska veza se, zbog znatno nižih troškova, preporučuje malim prodavnicama.

Za unos podataka u bankomat koriste se čitač kartice i tastatura. Informacije sačuvane na magnetnoj traci smeštenoj na poledini kartice očitavaju se čitačem kartica i prosleđuju centralnom računaru. Tastatura vlasniku kartice služi da bi, pre svega, odabrao vrstu transakcije, a zatim i iznos. Početni korak prilikom upotrebe bankomata jeste unošenje ličnog identifikacionog broja (PIN) koji se u šifrovanom obliku šalje centralnom računaru. Identifikacioni broj se mora uneti pažljivo, jer bankomati nakon tri neispravna pokušaja unosa broja uglavnom blokiraju karticu.



Slika 5: Izgled bankomata

Bankomati imaju četiri izlazna uređaja: zvučnik, monitor, štampač i kasetu za novac. Prilikom unosa podataka, svaki pritisak korisnika na taster izaziva kratak zvučni signal, koji ga obaveštava o tome da je uneo podatak. Tokom transakcije, na monitoru se ispisuju uputstva po kojima korisnik treba da postupa da bi je uspešno doveo do kraja. Nakon što uzme novac, korisnik dobija potvrdu o obavljenoj transakciji odštampanu na matričnom ili termalnom štampaču. Najvažniji deo svakog bankomata sačinjavaju kasete za novčanice i mehanizam za brojanje novčanica. U zavisnosti od modela, bankomati mogu imati jednu, dve ili četiri kasete, sa sigurnosnom bravom ili bez nje. Foto-čelija registruje svaku novčanicu koja izađe iz kasete, a broj novčanica i informacije o svakoj pojedinačnoj transakciji čuvaju se u izveštaju, koji se periodično štampa. Kada se izdvoje iz kasete, novčanice se prenose do točka za razvrstavanje, gde se slažu u svežanj za izdavanje. Debljina svake novčanice meri se posebnim senzorom. U slučaju da su dve novčanice zalepljene jedna za drugu, mehanizam za brojanje ih prosleđuje u kasetu za odbačene novčanice. U tu kasetu se prosleđuju i pohabane, pocepane ili savijene novčanice koje automat ne može ispravno da

prepozna. Podaci o broju odbačenih novčanica takođe se čuvaju u izveštaju, tako da vlasnik bankomata ima uvid u kvalitet korišćenih novčanica. Veliki broj odbačenih novčanica može ukazivati na problem s njihovim kvalitetom ili mehanizmom za brojanje.

Neki modeli bankomata imaju kasetu za nepodignute novčanice u koju se odlažu one koje korisnik, nakon obavljene transakcije, ne preuzme u određenom vremenu. Pojedini modeli imaju sličnu proceduru i za elektronske kartice koje korisnik odmah ne izvuče iz čitača - bankomat jednostavno "usisa" karticu. Osim ovih delova, manje-više uobičajenih za sve modele bankomata, proizvođači se trude da privuku kupce raznovrsnom dodatnom opremom. Zavisno od proizvođača, bankomat se može opremiti tastaturom prilagođenom slepim osobama, alfanumeričkom tastaturom, opremom za video konferencijsku vezu, sigurnosnom kamerom, modulima za isplatu kovanica, sistemom za rashlađivanje (kada se uređaj nalazi u zatvorenom prostoru), kasetama za stranu valutu koje se mogu podešavati, višenamenskim kasetama, kasetama sa automatskim pakovanjem, monitorom s filtrom koji odbija sunčevu svetlost, uređajem za besprekidno napajanje itd.

Najnoviji modeli bankomata, u stvari su kombinovani uređaji za polaganje i podizanje novca. Uplaćene novčanice prolaze kroz proceduru provere originalnosti i kvaliteta i potom se šalju u kasete za isplate. Na ovaj način se znatno produžava vreme ponovnog "punjenja" bankomata novčanicama.

3. Tipovi elektronskog bankarstva

3.1 Kućno bankarstvo (Homebanking)

Homebanking se definiše kao sistem za direktno korišćenje bankarskih usluga iz kuće, pošto omogućava neposredan transfer sredstava, informacija i naloga putem telefonske mreže, bez pisanja pratećih dokumenata. Aplikacija za homebanking komitentima banke pruža mogućnost da deo svojih poslova obave praktično "od kuće". Klijent banke koristi telefon, televizor ili kompjuter kao vezu ili telekomunikacioni link sa kompjuterskim centrom pomenute banke. Zaštita podataka banke od neovlašćenog pristupa sprovodi se instalacijom podataka homebanking-a na posebnom serveru. Ovaj server ima programe i bazu podataka samo za korisnike homebanking usluga i mora biti odvojen od Intranet mreže.

Osim zaštite podataka banke od neovlašćenog pristupa, vrši se i zaštita od neovlašćenog pristupa podacima u okviru same baze podataka za homebanking. Ovom vrstom zaštite štite se sami podaci baze podataka

homebanking-a, sa pravima pristupa, tj. samo vlasnik podataka može da vidi samo svoje podatke i da nikom drugom njegovi podaci nisu dostupni.

Ova vrsta zaštite je ostvarena korišćenjem lozinke (PIN-a) od strane svakog korisnika usluga kućnog bankarstva. Kod kreiranja ove lozinke primenjeni su slični algoritmi kao za kreiranje zaštite kod platnih karticaku. Ovakva zaštita obezbeđuje veliku sigurnost kod pristupa podacima.

Korisnik usluga homebankinga-a ima obavezu da se registruje sa svojim identifikacionim podacima (lični broj, ime i prezime i adresa) ako je građanin, a ako je firma sa identifikacionim podacima firme (matični broj, naziv firme, adresa). Na osnovu unetih identifikacionih podataka pisanim putem u zapečaćenoj koverti korisniku se dostavlja lozinka (PIN) i uputstvo za dalji rad.

Kod kućnog bankarstva razlikujemo tri faze koje su se menjale u zavisnosti od oblika telekomunikacionih veza između banke i klijenta, i to:

- Telefonsko bankarstvo;
- On-line bankarstvo (Kućno bankarstvo na bazi Intraneta);
- Internet bankarstvo (Internet Banking).

Telefonsko bankarstvo se u svetu javilo 70-tih godina prošlog veka. Ono omogućava telefonsko dobijanje informacije o stanju na računu, kao i davanje naloga za plaćanje. Usluga ce biti omogućena klijentu u toku zvaničnog radnog vremena banke, pri čemu klijent treba da informiše telefonskog operatera o broju svog računa i sigurnosnom kodu.

Moguća su dva načina obavljanja pomenute operacije:

- Komitent stupa u direktnu vezu sa službenikom banke i tada inicira operacije na bankarskom računaru;
- Komitent uspostavlja direktnu vezu sa bankarskim računarom.

U početnom periodu uvođenja kućnog bankarstva radi se isključivo o pružanju mogućnosti obavljanja plaćanja određenih periodičnih računa posredstvom telefona lociranog u stanu (Telephone Bill Payments –TBP). Kasnije sa uvođenjem video sistema dolazi do značajnog proširenja asortimana usluga (Video Home banking –VHB) zbog toga što korišćenje video teksta pruža dodatne tehničke prednosti: mogućnost korišćenja velikog broja kanala, porast brzine i pouzdanosti i mogućnosti proizvodjenja slike. Na taj način se komitentima obezbeđuje pregled informativnih stranica sopstvenih transakcija na posebno adaptiranim monitorima.

Sistem plaćanja preko telefona u suštini nije ništa drugo do obavljanje platnoprmetne operacije na bazi oralne instrukcije korisnika, preko transakcionog telefona. One se najčešće pojavljuju u dve tehničke vrednosti: u prvoj, komitent stupa u direktnu vezu sa službenikom banke i preko njega se iniciraju operacije bankarskom računaru; u drugoj, sam komitent uspostavlja direktnu vezu sa računarskim centrom banke.

Krajnji cilj ovih sistema je približiti uslugu klijentima i omogućiti im komunikaciju sa bankom ili drugom finansijskom institucijom od kuće, bez dodatnih napora u smislu odlaska na šalter banke ili posredne komunikacije. Sve veće prisustvo u domovima korisnika finansijskih usluga predstavlja polaznu osnovu homebanking sistema.

Razvoj telekomunacionog servisa u pravcu digitalizacije još više je otvorio vrata homebanking servisima u obliku digitalnih govornih tehnologija i sistema telefonskih govornih automata. S druge strane, globalizacija telekomunikacija preko postavljanja mreže svih mreža – Interneta, stvorila je preduslove za virtuelno bankarstvo od kuće.

3.2 On-line bankarstvo

On-line bankarstvo predstavlja obavljanje bankarskih transakcija direktnom vezom klijenta i banke uz pomoć specijalizovanog softvera. Dakle, potreban je poseban softver instaliran na klijentovom računaru sa kojim se jedino mogu obavljati transakcije i na kome će se nalaziti podaci o izvršenim promenama.

Pri obavljanju bankarskih transakcija u on-line bankarstvu:

- potreban je specijalan softver (Microsoft Money, Manage Your Money...) koji se ugrađuje u računar klijenta;
- klijent je ograničen na obavljanje transakcija sa sopstvenog računara;
- klijent posluje sa dve strane: sa bankom i softverskom kompanijom koja instalira i održava softver;
- klijentovi podaci o bankarskim transakcijama ostaju na hard disku i nisu otporni na eventualne napade iz okruženja (mogućnost pljačke, ubacivanje kompjuterskih virusa...);
- potreban je novac za kupovinu softvera;
- potrebno je vreme za instaliranje softvera, kao i vreme za ovladavanje programima.

Usluge koje su 24 sata dnevno dostupne su:

- pristup stanju na tekućem računu i kreditnim karticama;
- plaćanje računa;

- planirano i zakazano plaćanje za određeni termin koje će se izvršiti automatski;
- prenos novca sa računa na račun;
- usluge vođenja finansija za šta je potreban dodatni softver.

Nedostaci on-line bankarstva, poput ograničenja za obavljanje transakcija sa samo onog računara na kome je instaliran skup softver, potrebno vreme za obuku za rad, kao i nezaštićenost podataka na hard disku korisnika na napade iz okruženja, okrenuli su veliki broj korisnika ka Internet bankarstvu.

3.3 Internet bankarstvo

Internet sve značajnije utiče na način savremenog poslovanja i donosi nove izazove pred današnje banke. Postoji veliki broj zahteva koje treba ispuniti u cilju postizanja uspešnog poslovanja na Internetu, kao na primer, lakoća korišćenja aplikacija, sigurnost ličnih informacija, integracija sa postojećim sistemima, prihvatanje standarda otvorenih sistema...

Internet bankarstvo ili sajber bankarstvo (eng. Cyber Banking) predstavlja obavljanje bankarskog poslovanja direktno iz kuće, posredstvom Interneta.

Za obavljanje bankarskih transakcija u Internet bankarstvu nije potreban specijalan softver i ne postoje podaci uskladišteni na klijentovom hard disku, takođe, mora se naglasiti i da je pristup banci i računu moguć sa bilo kojeg mesta na svetu, pod uslovom da na tom mestu postoji računar i da je priključen na Internet. Banka brine o održavanju sopstvenog hardverskog i softverskog sistema zaštite.

Internet nudi bankama niz mogućnosti. Predviđanja su da će se ovaj vid bankarstva razvijati velikom brzinom. Internet bankarstvo je najjeftiniji oblik bankarskih usluga, dostupan 24 sata dnevno, praktično bez prostorne ograničenosti.

Glavni ograničavajući faktori, koji uslovljavaju pristanak potrošača na ovu vrstu tehnologije su sigurnost i privatnost. Sa tehničke tačke gledišta, ovaj problem su neke banke već rešile, ali ostaje činjenica da je ponašanje potrošača vođeno pre potrošačkom percepcijom nego tehničkom činjenicom. Neprihvatanje da se bankarske transakcije obavljaju preko interneta postoji pre svega iz straha da ključne finansijske informacije mogu da budu otkrivene.

Jasno su vidljive razlike između Internet bankarstva i on-line bankarstva. Osnovna razlika je u ugradnji specijalnog softvera, koji ograničava korisnika na obavljanje usluga isključivo sa računarom u koji je ugrađen taj softver.

Razlike su i u stepenu sigurnosti pri obavljanju transakcija, zatim u novcu potrebnom za kupovinu i ugradnju softvera i vremenu potrebnom za obuku korisnika. Pomenuti razlozi jasno ukazuju da je Internet bankarstvo praktičniji, ekonomičniji i bezbolniji način obavljanja bankarskog poslovanja direktno iz kuće.

Razlozi zbog kojih se banke pojavljuju (rade) na Internetu su sledeći:

- Stvaranje imidža inovativne firme, koja je u stanju da svojim korisnicima ponudi najsavremenija tehnološka rešenja.
- Bolje i veće interaktivne mogućnosti. Za banku koja se u tržišnim uslovima bori za svakog svog komitenta, najvažnija je komunikacija sa njim. U klasičnim uslovima banka je mogla da komunicira samo dok je trajalo radno vreme, ili preko nekog informativnog šaltera koji bi radio neprekidno. Ovakav način poslovanja stvarao je ograničenja u komunikaciji. Interaktivne mogućnosti komuniciranja preko Interneta su praktično neograničene i samo je pitanje do kog nivoa banka ima interesa da se angažuje.
- Mogućnost racionalizacije potencijala banke. Banka prenošenjem određenih servisa na Internet redukuje troškove poslovanja, jer ne mora za povećanje broja komitenata, da otvara novi poslovni prostor, da ga oprema i zapošljava nove službenike. Ovo je posebno interesantno za one geografske regione gde banka nema mrežu ekspozitura ili ima mali broj komitenata. Sa Internetom banka može da pokrije znatno veći geografski prostor ne otvarajući nove ekspoziture. Veliki broj informacija koje banka može da stavi svojim korisnicima na raspolaganje u principu nisu dostupni širem krugu njenih korisnika. To se odnosi na mogućnosti plasmana i kreditiranja po najpovoljnijim uslovima, inostrana plaćanja, savetodavne funkcije i dr.
- Samouslužno bankarstvo je korisno, podjednako i za banku i za korisnika, jer korisnik ima servise 24 časa dnevno, 7 dana u nedelji, a banka bez povećanja broja zaposlenih radi 24 časa dnevno.
- Banka, svojom pojavom na Internetu dokazuje svoje konkurentne mogućnosti i svoj razvoj, kao solidna, stabilna i tehnološki napredna firma.

Iskustva naprednijih zemalja pokazuju da banka bez razvijenog sistema elektronskog bankarstva više neće biti u stanju da preživi. Razlog za to jeste konkurentna ponuda, odnosno potreba za kvalitetnijim finansijskim servisom.

Sa stanovišta konzumenata bankarskih usluga, za očekivati je da niži troškovi banke rezultuju višim kamatama na depozite, nižim provizijama na usluge i posebno mogućnost plaćanja on-line. Nimalo nije beznačajno što se

ne mora čekati u redovima, trošiti vreme i sve to samo u radno vreme bankarskih šaltera.

Banke su po prirodi konzervativne institucije. U početku su banke ostale po strani, ali sagledavanjem prednosti, a i problema, krenule su najpre samo sa informacijama, zatim na dvosmernu komunikaciju, a u trećem koraku i na transakcije.

- Informativno predstavljanje je jednosmerna komunikacija gde se banke preko Interneta samo predstavljaju svojim – postojećim ili novim, potencijalnim korisnicima. Uglavnom ima reklamni karakter. Većina banaka je to uradila.
- Dvosmerna komunikacija korisnika i banke – putem e-maila ili interaktivnim pristupom nekom servisu. Ovo su takođe podaci marketinškog karaktera, ali postoji mogućnost, uz korisnikovu identifikaciju i autentifikaciju, da mu banka stavi na raspolaganje i dodatne informacije, servise.
- Bankarske transakcije na Internetu su najviši nivo komunikacije banke i komitenta.

Banke su shvatile da nije dovoljno da imaju samo Internet prezentacije koje dobro izgledaju. Danas se postavljaju dodatni zahtevi da prezentacije moraju da pruže i nešto više, da budu interaktivne, multimedijalne i da omogućavaju kompletno poslovanje direktno na Internetu. Zbog toga su banke u svoje Internet poslovanje uvele niz inovacija (virtualne poslovnice, specijalne finansijsko-softverske programe koji brinu o budžetu klijenata, ulaganjima...). Ipak i pored pomenutih inovacija ponuda bankarskih proizvoda i usluga je gotovo uniformna.

Bankarski proizvodi i usluge koje nudi većina svetskih banaka u svom Internet poslovanju su:

- menjački poslovi
- otvaranje i korišćenje zajmovnog računa (Loan account)
- provera stanja na računima klijenta
- otvaranje i korišćenje čekovnih računa
- plaćanje računa elektronskim putem
- korišćenje sistema kreditnih kartica (Visa, Master Card...)
- trgovina hartijama od vrednosti
- obustave plaćanja (Stop Payment)
- otvaranje i korišćenje tekućih računa
- provera transakcija iz prethodnog perioda na svim računima klijenta
- elektronski transferi između računa

- e-mail korespodencija (dostavljanje svih najvažnijih informacija za klijentovo poslovanje poput: informacije sa svetskih berzi, informacije o aktivnostima banke, informacije o stanju klijentovih ulaganja...)
- otvaranje i korišćenje depozitnih računa
- odobravanje hipotekarnih i ostalih kredita
- savetodavna funkcija

Bankarsko poslovanje na Internetu je brzo, efikasno i ekonomično. Otvaranje računa u Internet bankama je potpuno besplatno. Provizije za plaćanje računa elektronskim putem su minimalne ili u većini banaka potpuno besplatne. Ostale provizije za Internet bankarske proizvode i usluge su identične ili manje od provizija u takozvanom tradicionalnom (filijalnom) bankarstvu.

Plaćanje računa preko Interneta elektronskim novcem ili pametnim karticama (Smart Cards) je nova aktivnost koju Internet banke omogućavaju svojim klijentima.

Prednosti Internet bankarstva

Internet bankarstvo ima niz prednosti u odnosu na takozvano tradicionalno poslovanje banaka. Prednosti se uglavnom ogledaju u vremennoj i prostornoj neograničenosti, brzini obavljanja transakcija, niskoj ceni i širokom asortimanu bankarskih proizvoda i usluga.

Radno vreme Internet banaka

Osnovna prednost Internet banaka je njihovo neograničeno radno vreme. U tradicionalnom bankarstvu za obavljanje bankarskih usluga non-stop bilo bi potrebno angažovati tri smene ljudi da svakodnevno radi 365 dana u godini i to u široko razgranatoj bankarskoj mreži. Potreban broj ljudi za obavljanje non-stop poslovanja bio bi veoma velik, kao i troškovi ovakvog načina poslovanja.

Prostorna neograničenost Internet bankarstva

Većina ljudi bira banku zbog blizine. Danas ljudi mogu imati banku unutar svog doma, bez obzira gdje god da žive. Internet bankarstvo je moguće obavljati sa bilo kog mesta na svetu. Potrebno je da korisnik ima otvoren račun u nekoj banci koja pruža usluge Internet bankarstva, da na mestu iz kog obavlja poslovanje postoji računar sa pristupom Internetu i da korisnik zna sve šifre koje su mu potrebne za ulazak u Internet banku i njegov račun. U klasičnom bankarstvu korisnik je vezan za mesto i zemlju gde postoji filijala banke u kojoj ima otvorene račune.

Brzina obavljanja transakcija

U klasičnom bankarstvu potrebno je utrošiti vreme za dolazak i odlazak u filijalu banke, zatim vreme za čekanje u filijalama, vreme za popunjavanje obrazaca, čekova i ostalih dokumenata, kao i vreme za obavljanje samih transakcija. Internet bankarstvo je daleko brži način za obavljanje bankarskog poslovanja. Za poslovanje u Internet banci potrebno je samo vreme za prijavljivanje u Internet banku i vreme za obavljanje bankarske transakcije.

Cena obavljanja bankarskih transakcija

Internet bankarstvo je najjeftiniji oblik obavljanja bankarskih transakcija. Provizije koje se plaćaju za obavljanje bankarskih usluga u Internet bankarstvu su iste ili niže od onih u tradicionalnom bankarstvu. Za obavljanje kvalitetnog bankarskog poslovanja u tradicionalnom bankarstvu je potrebno daleko više ljudi, poslovnog prostora i opreme, nego u Internet bankarstvu. Samim tim i troškovi obavljanja bankarskog poslovanja u tradicionalnom bankarstvu su daleko veći od onih u Internet bankarstvu.

Nedostaci Internet bankarstva

Nedostaci Internet bankarstva najviše su izraženi u smanjenoj sigurnosti pri obavljanju poslovanja, nepostojanju zakonske regulative, nedostatku privatnosti, otuđenosti i odbojnosti prema inovacijama i opasnosti od zloupotrebe Internet bankarstva u kriminalne svrhe.

Sigurnost, odnosno nedostatak sigurnosti i sistemi zaštite na Internetu su ključni faktor rasta i razvoja Interneta. Ti faktori su veoma važni za funkcionisanje i razvoj Internet bankarstva.

Sa rastućim publicitetom otvorenih mreža kao što je Internet i elektronskom razmenom informacija i novca između geografski udaljenih lokacija, obezbeđenje transakcija postaje od ključne važnosti. Banke koje koriste elektronsku razmenu podataka u zatvorenim mrežama (intranet) osiguravaju se utvrđivanjem identiteta i autorizacijom ljudi koji pristupaju mreži. U otvorenim mrežama, postojeći mehanizmi tehničke i pravne zaštite nisu dovoljni da spreče neautorizovan pristup i hakerske upade. Određenim kriptografskim tehnologijama koje uključuju digitalni potpis, definiše se nova infrastruktura čija je osnovna prednost viši nivo integriteta poruke i verifikacija pristupa.

Ovom tehnologijom šifrovanje poruke obezbeđuje dve stvari za učesnike u razmeni:

- da je njihova poruka osigurana i
- da je druga strana autorizovana za pristup.

Šifrovanu poruku je teško falsifikovati, pa se očekuje da će tehnologija digitalnih potpisa biti primenjena i prilikom zaključivanja ugovora elektronskim putem.

Nepostojanje zakonske regulative

Globalni sistem komuniciranja, kakav je Internet, zahteva ažurne i adekvatne pravne okvire koji treba da definišu potrebe poslovnih subjekata i korisnika usluga. Zakonska regulativa u vezi Interneta i poslovanja na njemu, razlikuje se od zemlje do zemlje. Dva ekonomski najrazvijenija dela svijeta, SAD i Evropska unija imaju različite stavove po pitanju zakonske regulative na Internetu. Evropska unija ima daleko liberalnije stavove po pitanju privatnosti poslovanja od SAD. Usaglašavanje njihovih stavova o zakonskoj regulativi na Internetu, od velikog je značaja za kompletnu svetsku privredu.

Postoje dva moguća scenarija za rešenje zakonske regulative u poslovanju na Internetu.

Prvi scenario, za koji se zalaže Evropska unija, je liberalnog tipa i zasniva se na potpunoj anonimnosti i privatnosti poslovanja.

Drugi scenario, za koji se zalažu SAD, je zasnovan na kompletnoj kontroli poslovanja, transakcija i podataka od strane državnih organa.

Potpuno anonimni sistem poslovanja na Internetu moguć je zahvaljujući sistemu šifrovanja podataka, uz pomoć koje je zagarantovana anonimnost u slanju svih poruka na Internetu. Na ovaj način, sistem štiti privatnost poslovanja pojedinca ili preduzeća, što je ujedno i osnovno pravilo bankarskog poslovanja i dobra strana ovog sistema. Sa druge strane, mane ovog sistema su što omogućavaju izbegavanje plaćanja poreza, carinskih obaveza, pranje novca i prebacivanje kapitala u druge zemlje i to mimo znanja finansijskih, carinskih, poreskih i ostalih državnih organa. Potpuno anonimni sistem Internet poslovanja, uz odsustvo zakonske regulative mogao bi uzdrmati ne samo državne organe, nego i čitav bankarski sistem najrazvijenijih zemalja sveta. Bankarski sistem SAD i Evropske unije bi bili ugroženi zbog odliva velike količine kapitala u takozvane Off-Shore bankarske centre. To je doprinelo da Internet banke sa područja SAD mogu poslovati samo sa rezidentima SAD, unutar bankarskog sistema SAD i isključivo u američkim dolarima.

Drugi sistem rešenja zakonske regulative za poslovanje preko Interneta, zasniva se na kompletnoj kontroli i evidenciji transakcija, poslovanja, i podataka na Internetu od strane državnih organa. Ovaj sistem bi omogućavao državnim organima kompletan uvid u svačiji bankovni račun, u sve Internet transakcije i e-mail korespondenciju. Sloboda i privatnost pojedinca kao i osnovna pravila poslovnog i bankarskog ponašanja ovim sistemom bi bila prekršena na najgori mogući način.

Pred vladama najrazvijenijih zemalja je zadatak da se slože da li da redizajniraju monetarni i poreski sistem u skladu sa nastalim tehnološkim promenama ili da naprave sistem u kome bi svako ulaganje, svaka kupovina, svaka transakcija svakog pojedinca i preduzeća bila praćena tokom čitavog života.

Oba prikazana sistema imaju svoje dobre i loše strane. Kombinovanjem njihovih najboljih elemenata, dobilo bi se optimalno rešenje zakonske regulative za poslovanje na Internetu. Sigurno je da će još dosta vremena proći dok se ne usaglasе međudržavne zakonske regulative vezane za poslovanje pojedinaca i preduzeća na Internetu. Do tada, nedostatak međudržavne zakonske regulative onemogućavaće određene segmente poslovanja, dok će sa druge strane omogućavati primenu širokog spektra nezakonitih aktivnosti u poslovanju pojedinaca i preduzeća na Internetu.

Odbojnost prema inovacijama kao prepreka u razvoju Internet bankarstva

Inovacije i nove proizvode većina ljudi prihvata sa izvesnom dozom nepoverenja i nezainteresovanosti. Identična situacija je i sa Internetom i poslovanjem na njemu. Internet kao potpuno novi vid komuniciranja, u početku je prihvatio samo veoma uzak krug ljudi, inovatora i to prvenstveno naučnika, vojnih lica i univerzitetskih profesora. Vremenom je sve više ljudi koristilo Internet i pogodnosti koje on pruža. Biće potrebno još mnogo godina dok se Internet i poslovanje na njemu prihvati i implementira u svim delovima sveta.

Sigurnost i sistemi zaštite poslovanja Internet banaka

Bankarske institucije koje svoju delatnost obavljaju na Internetu suočene su sa ozbiljnim problemima zaštite obavljanja bankarskih transakcija. Ne postoje savršeni sistemi zaštite. Internet banke kao i tradicionalne banke mogu biti opljačkane. To svakako nije razlog zbog koga bi ljudi prestali da ulažu u banke. Naprotiv, osnova bankarskog poslovanja je poverenje. Klijenti imaju povjerenje u Internet banke, jer kao i ostale finansijske institucije one garantuju svojim klijentima naknadu sredstava u slučaju pljačke. Internet banke nastoje da razviju još savršenije sisteme zaštite.

3.4 Mobilno bankarstvo

Mobilno bankarstvo (Mobile Banking) je najnoviji trend u razvoju elektronskog bankarstva. Konvergencija mobilnih komunikacija i Interneta otvara nove kanale za različite finansijske servise. Finansijske institucije sada imaju mogućnost da ponude bankarske, brokerske, usluge osiguranja preko mobilnih telefona, personalnih digitalnih asistenata (PDA) ili pejdžera. Pri tom one povećavaju lojalnost svojih klijenata kao i produktivnost svojih zaposlenih.

Broj finansijskih servisa u velikoj meri zavisi od raspoložive mobilne platforme na kojoj će se izvršavati. Danas imamo različite vrste finansijskih servisa i možemo ih podeliti na: bankarske, brokerske, servise investicionog bankarstva i druge finansijske servise.

Skoro sve veće banke su uvele ili planiraju da lansiraju servise mobilnog bankarstva. Dok je većina starijih aplikacija realizovana kao SMS, dvosmerni komunikacioni protokol, većina današnjih aplikacija bazirana je na WAP standardu (Wireless Applications Protocol). WAP omogućava mobilnim uređajima da komuniciraju preko Interneta jednostavnim unošenjem adrese kojoj žele da pristupe. Raniji servisi bili su tipično informaciono-bazirani, korisnici su mogli da putem svog mobilnog uređaja proveravaju stanje na računu, proveravaju stanje svoje kreditne kartice ili da dobiju neke osnovne finansijske informacije. U novijem vremenu banke su počele da objedinjuju mogućnosti transakcija u svojim servisima. Od ovih servisa najčešće se koriste plaćanje računa, prenos sredstava ili aplikacije kreditiranja.

Servisi mobilnih plaćanja su još uvek u fazi razvoja. Za sada još uvek nema najboljeg rešenja koje bi zadovoljilo kritičnu masu korisnika i koje bi se nametnulo kao standard na tržištu. Razvoj mobilnog plaćanja će se nastaviti sve dok se ne iskristališe jedno ili dva rešenja koja će se nametnuti kao standard na tržištu.

Prvi pokušaji mobilnog plaćanja obuhvatali su standardne bankarske kreditne i debitne kartice u integraciji sa mobilnim telefonom. Postupak plaćanja bio je sledeći. Korisnici su pomoću telefona ili Interneta naručivali proizvode, preko svog mobilnog telefona primali su SMS poruku o uspešnoj narudžbini a zatim su kompletirali transakciju tako što su ubacivali karticu u čitač i unosili šifru. Međutim kompanije bi morale da ponude integrisano rešenje mobilnih uređaja i čitača kartica. Prednost je naravno stepen sigurnosti koji je u ovom slučaju izuzetno visok i vezan za čitača kartica.

Kompanije takođe nude usluge mobilnog plaćanja za koje nije potrebna upotreba smart kartica. Korisnici obavljaju transakcije tako što unose poseban broj koji se odnosi na recimo parking servis ili bilo kojeg drugog pružaoca usluga. Operater mobilne telefonije u ovom slučaju igra ulogu klirinške kuće, on kreditira korisnikov unapred određeni račun. Ovakvo rešenje je veoma dobro za mikro plaćanja kao što je plaćanje različitim trgovcima. Ovakve aplikacije plaćanja bez upotrebe kreditnih kartica su veoma privlačne za korisnike pošto omogućavaju klijentima i trgovcima da obavljaju transakcije upotrebom postojeće infrastrukture. Nema nikakve potrebe da pojedinac kupuje posebne uređaje ili da kompanije ulažu dodatne investicije u svoju opremu. Najvažniji nedostatak ovakvog oblika plaćanja je sigurnost. Postojeće rešenje se oslanja na sigurnost GSM mreže koja sama po sebi nije dovoljna da spreči zloupotrebe prilikom transakcija.

Bluetooth tehnologija koja omogućava uređajima da na malim razdaljinama komunicira pomoću brzih radio signala takođe može da odigra važnu ulogu u sistemima mobilnog plaćanja. Pomoću bluetooth tehnologije korisnici mogu da obavljaju različite vrste mikro plaćanja tako što će svoj mobilni telefon prineti uređaju za plaćanje i tako obaviti transakciju.

Mobilni keš predstavlja način punjenja mobilnih telefona »kešom« najčešće pomoću smart kartica. Koncept je još uvek u eksperimentalnoj fazi i još uvek nema jedinstvenog procesa koji bi se nametnuo kao standard u ovoj oblasti.

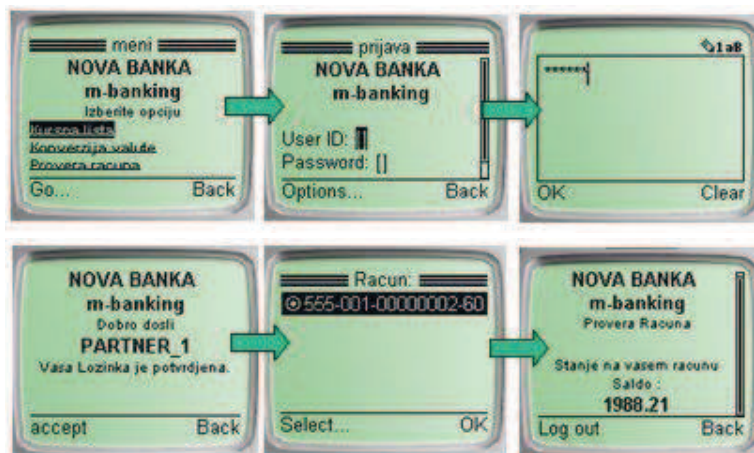
Tehnička infrastruktura mobilnog bankarstva obuhvata sledeće:

- Mobilni uređaji - Svaki od mobilnih uređaja zahteva određeni način komunikacije, oni zahtevaju sopstveni gateway za komunikaciju sa aplikativnim serverom. Svaki ima različitu veličinu ekrana prilagođenu različitim vrstama prikaza podataka. Različite tastature generišu i različite sisteme navigacije sa aplikacijom. Izazov za aplikativni server je da razvrstava ove uređaje i da svakom šalje podatke u formatu koji će biti u skladu sa njihovim dizajnom.
- Povezivanje, Gateway - Polazeći od krajnjeg korisnika, mobilni uređaj može biti bilo koji uređaj kojim on prustupa lokalnom cell centru. Cell centar odgovara za pokrivenost određenog geografskog regiona. Kada primi podatke on ih šalje baznoj stanici. Mobilna mreža snima i identifikuje sve potrebne informacije u lokalnom registru, ukoliko je korisnik na lokalnoj geografskoj pokrivenosti. Ako nije tada stanica prati poziv, tada se određuje roaming poziva.
- Bežični srednji sloj (aplikativni sloj) - Aplikativni sloj je centralni deo mobilnog sistema. To je mesto gde se tok podataka kontroliše, postavljaju pravila, i izvršavaju fajlovi. Aplikativni softver bi trebalo da bude otvoren sistem koji lako može da uspostavi komunikaciju sa

drugim sistemima. Jedan od najčešćih metoda komunikacije sa back-end sistemima je XML-API alat za rad sa podacima.

Sigurnost je jedan od najvažnijih zahteva mobilnog bankarstva, ako ne i najvažniji. Istraživanja pokazuju da kod mobilnog bankarstva kao i kod on-line bankarstva korisnici imaju malo poverenja u bezbednost aplikacija. Efikasan, za sada standardni način zaštite podataka na internetu je primena tehnike javnih ključeva (Public Key Infrastructure) PKI, u osnovi obuhvata privatni i javni kluč koji između sebe dele učesnici u komunikaciji. Treći element, digitalni sertifikat, je potpisan od treće strane koja je autorizovana za izdavanje sertifikata.

Jedan primer aplikacije u mobilnom bankarstvu je dat na slici. Aplikacija omogućava korisniku da preko svog mobilnog uređaja pogleda najnoviju kursnu listu, izvrši konverziju željene valute ili pogleda stanje na svom žiro računu. Ovakva aplikacije može biti od velike koristi ako se recimo nalazite na odmoru a istovremeno očekujete da vam stigne neka uplata. Ukoliko želi da pogleda stanje na svom žiro računu korisnik prvo mora da izvrši identifikaciju tako što unosi svoj identifikacioni broj i password.



Slika 6: Aplikacija u mobilnom bankarstvu

Ukoliko je identifikacija uspešna korisnik dobija spisak svojih žiro računa. Na ovaj način aplikacija je pojednostavljena jer korisnik ne mora da unosi broj računa preko tastature, takođe je eliminisana mogućnost greške koja bi nastala usled pogrešno ukucanog broja. Nakon selektovanja žiro računa korisnik na ekranu mobilnog uređaja dobija uvid u stanje na tom žiro računu.

Prognozira se da će mobilno bankarstvo doživeti čak i snažniju ekspanziju od Internet bankarstva u narednih tri do pet godina, s obzirom na to da broj korisnika mobilnih telefona daleko prevazilazi broj korisnika Interneta.

4. Identifikacija i analiza rizika u e-bankarstvu

Brze promene u informacionim tehnologijama koje utiču na prilagođavanje bankarske tehnologije u sferi e-bankarstva i e-novca, u značajnoj meri utiču da lista rizika nikada ne može biti potpuna. Specifični rizici sa kojima se e-banke suočavaju u oblasti e-bankarstva i e-novca, mogu se grupisati na sledeći način:

- Operacioni rizik koji može biti:
 - Rizici sigurnosti - pojavljuju se u vezi sa kontrolom: sistema računovodstva, informacija pomoću kojih banka komunicira sa okruženjem, transfera e-novca, kao i sprečavanja pronevera - falsifikata.
 - Rizici dizajniranja sistema, implementacije i održavanja - predstavlja ključnu fazu razvoja sistema e-bankarstva i e-novca. Zbog toga se rizici koji mogu nastati neadekvatnom pripremom ove faze, mogu manifestovati u prekidu ili usporavanju sistema.
 - Zloupotreba proizvoda i usluga od strane korisnika - rizik ove vrste se povećava kada banke neadekvatno edukuju korisnike u pogledu mera sigurnosti prilikom verifikacije transfera e-novca.
- Reputacioni rizik - Odnosi se na negativne posledice javnog mnjenja za banku, koji rezultira u gubitku obezbeđivanja sredstava za finansiranje ili gubljenju korisnika usluga. Može nastati zbog: neupoznatosti korisnika sa potrebnim informacijama o korišćenju usluga, zbog bankarskog prestupa, malverzacije i obmana treće strane, zbog ponude istih ili sličnih proizvoda e-bankarstva i e-novca...
- Pravni rizik - Nastaje kada prava i obaveze strana koje učestvuju u finansijskim transakcijama nisu do kraja pravno regulisane, pri narušavanju pravila, propisa, nepoštovanje zakona...
- Tradicionalni bankarski rizici – Odnose se na:
 - Kreditni rizik-odnosi se na korisnika kredita i mogućnost da se ne izvrši obaveza u pogledu iznosa otplate kredita ili roka otplate.
 - Rizik likvidnosti-nastaje kada banka nije u mogućnosti da izvršava dospele obaveze koje nastaju u uslovima e-poslovanja

- Rizik kamatne stope- odnosi se na smanjenje kamatnih stopa do stepena u kome negativna kretanja kamatnih stopa smanjuju vrednost imovine u zavisnosti od neispunjenih obaveza u e-novcu.
- Tržišni rizik- je rizik gubitka, posebno u delu vanbilansnih pozicija, koji proističe iz kretanja cena.

Rizici internacionalnog e-poslovanja - E-bankarstvo i e-novac ne poznaju geografske barijere, tako da se tržišna ekspanzija širi izvan nacionalnih granica.

5. Istraživanje trenda razvoja mobilnih plaćanja

Demografsko i metodološko istraživanje je sprovedeno od strane istraživačke kuće KPMG u periodu od septembra 2010 do februara 2011 godine na ukupno 970 kompanija širom sveta, online anketom kako bi se ispitao stav i zrelost po pitanju upotrebe mobilnog plaćanja .

Fokus istraživanja u anketi je davanje odgovor na sledeća pitanja:

- Mobilna plaćanja i njen poslovni uticaj;
- Usvajanje tehnologija, aplikacija i usluga za mobilna plaćanja;
- Strategija korišćenja mobilnih plaćanja, mogućnosti i prepreke;
- Ključni korisnici sistema mobilnog plaćanja;

Ovim istraživanjem su obuhvaćene finansijske aktivnosti, plaćanje robe i usluga, zatim mobilno bankarstvo, sa fokusom isključivo na mobilna plaćanja. Kompanije su industrijski povezane po svim regionima i predstavljaju poslovne jedinice koje imaju udeo u mobilnom ekosistemu plaćanja.

Isto kao što poslovanje ima različite vidove i oblike plaćanja, mobilno poslovanje ima više značenja i mobilna plaćanja mogu imati različite forme. U istraživanju kompanije su pitane da ocene prosperitet različitih oblika mobilnih plaćanja:.

- M-novčanik: informacije o računima i transakcijama su uskladištene na SIM kartici;
- M-bankarstvo: direktni pristup izdavaocu bankarskih servisa i informacija putem mobilnih telefona;
- Bezkontaktni sistemi kartica: bežična komunikaciona tehnologija na malom rastojanju upotrebom radio talasa visoke frekvencije, koja omogućava razmenu podataka između uređaja;
- Specijalizovani onlajn sistemi: na primer PayPal, MoneyBookers.

- Naplata putem posrednika: na primer: SMS parking, račun je fakturisan na računu pretplatnika za mobilni telefon.

Po datom istraživanju jedino M-bankarstvo i specijalizovani onlajn sistemi imaju trenutno vodeću poziciju u mobilnim plaćanjima. Kod preostalih rešenja, ispitanici su uglavnom odgovorili da je suviše rano predvideti da li će neko rešenje biti šire prihvaćeno.

6. Obezbeđivanje sigurnosti transakcija na internetu

Internet tehnologija i protokoli podložni su mogućim napadima koji narušavaju bezbednost podataka i identiteta subjekata. U cilju rešavanja navedenih problema, uporedo sa razvojem računarskih mreža, razvijaju se i specijalizovani softverski i hardverski sistemi zaštite. Danas u svetu postoji veliki broj proizvođača tehnološki kvalitetnih proizvoda za različite nivoe zaštite savremenih mreža. U ovim proizvodima su ugrađeni javni standardni kriptografski algoritmi.

Najkvalitetnija kriptografska rešenja koja se primenjuju u savremenim računarskim mrežama baziraju se na primeni simetričnih kriptografskih sistema za zaštitu tajnosti, asimetričnih kriptografskih sistema baziranih na tehnologiji digitalnog potpisa, digitalnih sertifikata i hardverskih modula (kriptografski koprocesori i smart kartice). Ovakvi sistemi zaštite su projektovani da se uspešno odbrane od potencijalnih opasnosti i napada u cilju ugrožavanja bezbedno osetljivih resursa informacionih sistema.

Infrastruktura sistema sa javnim ključevima (*eng. Public Key Infrastructure - PKI*) predstavlja platformu koja omogućava korisnicima javnih mreža, kao što je Internet, sigurne transakcije podataka i novca.

Ključni aspekt PKI sistema je upravo **sigurnost** koje se postiže primenom asimetričnih i simetričnih kriptografskih algoritama. Kriptologija je termin koji potiče od grčkih reči *kriptos* (skriven, tajan) i *logos* (nauka) i označava discipline koja se bavi sigurnim komunikacijama.

Kriptografija podrazumeva metode i algoritme za obezbeđivanje tajnosti informacija, dok **kriptoanaliza** podrazumeva metode i algoritme za narušavanje tajnosti istih.

Osnovne funkcije kriptografije u PKI sistemima definisane su na sledeći način:

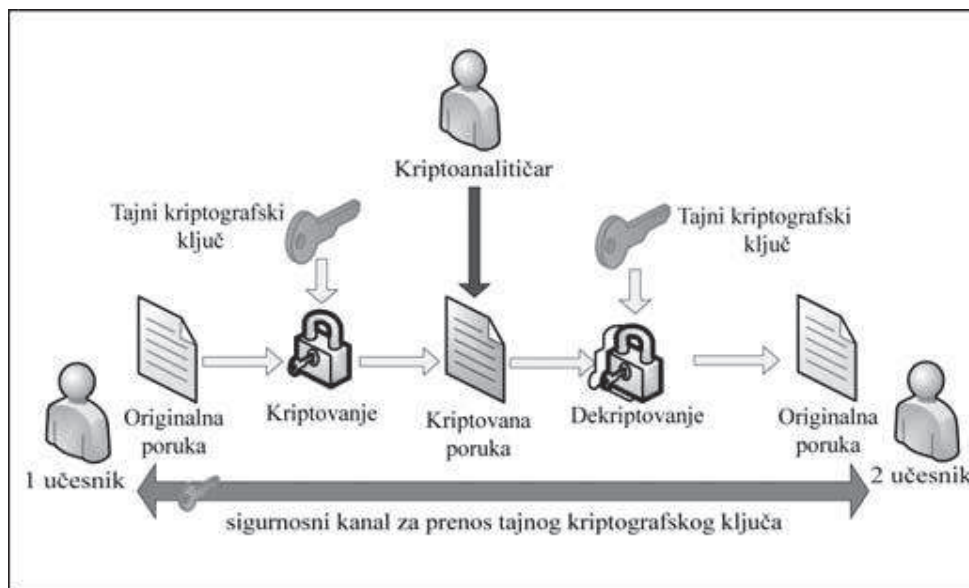
- zaštita tajnosti – informacije su dostupne samo ovlašćenim korisnicima,
- autentikacija – mogućnost provere i garantovanja identiteta učesnika u komunikaciji,

- integritet podataka – mogućnost otkrivanja neovlašćene promene podataka,
- neporecivost transakcija – sprečavanje mogućnosti poricanja realizacije određenih aktivnosti učesnika u komunikaciji (kao što su slanje poruke, transakcija i dr.).

Pored poznavanja kriptografskih metoda i algoritama uvođenje PKI sistema podrazumeva i upoznavanje sa direktivama, standardima i domaćim zakonodavstvom iz ove oblasti.

Posebno mesto u kriptografskim sistemima zauzimaju funkcije za kreiranje otiska (*eng. Hash functions*), koje su usko vezane za elektronsko potpisivanje dokumenta.

Simetrička kriptografija je najstariji oblik kriptografije. Osnovni simetrički kriptografski algoritam definisao je i 1949. godine predstavio C. Shannon. Ovaj način kriptografije podrazumeva poznavanje algoritma kojim se vrši kriptovanje i ključa kriptovanja koji sme biti poznat samo učesnicima u komunikaciji. Dakle svaka dva korisnika u komunikaciji moraju imati zajednički i jedinstveni **privatni ključ**.



Slika 7 : Princip rada simetričnog kriptografskog sistema

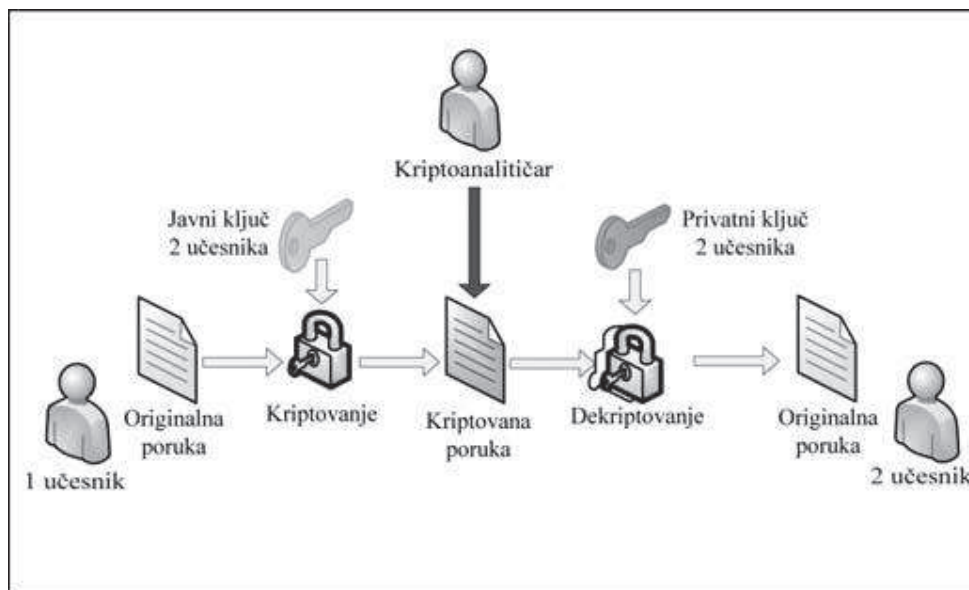
Osnovni nedostaci simetričke kriptografije su:

- problemi distribucije ključeva - kako dostaviti ključeve do strana koje komuniciraju, a da u procesu dostave ne budu kompromitovani

- veliki broj ključeva potreban za komunikaciju između više korisnika – naime za n učesnika u komunikaciji potrebno je $n(n-1)/2$ ključeva.

Asimetrični kriptografski algoritmi (eng. Asymmetric Key Algorithms) predstavljaju kriptografske algoritme kod kojih se za kriptovanje i dekriptovanje koriste različiti ključevi. Svaki učesnik u komunikaciji poseduje kriptografski par ključeva, tj. **privatni i javni ključ**. Javni ključ je dostupan svim učesnicima u komunikaciji, dok je privatni ključ poznat samo vlasniku ključa.

Komunikacija se uspostavlja korišćenjem unapred dogovorenog prenosnog komunikacionog kanala, a kriptovanje poruka koje se razmjenjuju vrši se korišćenjem prethodno razmenjenih javnih ključeva te privatnih ključeva koji su poznati samo vlasnicima tj. kreatorima pojedinačnih poruka. Princip rada asimetričnog kriptografskog sistema dat je na slici.



Slika 8: Princip rada asimetričnog kriptografskog sistema

Današnji PKI sistemi baziraju se na kombinaciji simetričnih i asimetričnih kriptografskih algoritama, kao i hash funkcija.

U PKI sistemima postoje dva opšta problema:

- količina podataka koje je potrebno kriptovati i
- vreme izračunavanja asimetričnih funkcija za kriptovanje.

Hash funkcije se svrstavaju u kriptografske algoritme bez ključa. Osnovna ideja hash funkcija je da naprave otisak dokumenta koji se kriptuje.

Osnovne karakteristike otiska su te da je znatno manji od originalnog dokumenta i da jednoznačno opisuje dokument.

PKI sistemi predstavljaju kombinaciju hardverskih i softverskih proizvoda, politika i procedura povezanih tako da omogućavaju korisnicima koji se ne poznaju ili nemaju mogućnost fizičkog pristupa jedni drugima da komuniciraju bezbedno kroz mrežu poverenja.

Poverenje u PKI sistemima bazira se na digitalnim sertifikatima. U praksi se koristi i termin digitalni identiteti (Digital ID). Digitalni sertifikati povezuju identitet korisnika sa njegovim digitalnim potpisom, a u praksi se koristi još i termin elektronski potpis.

Osnovne komponente PKI sistema su:

- **politika sertifikacije** (eng. *Certificate Policy - CP*),
- **praktična pravila rada** (eng. *Certificate Practice Statement - CPS*),
- **sertifikaciono telo** (eng. *Certificate Authority - CA*),
- **registraciono telo** (eng. *Registration Authority - RA*),
- **sistemi za distribuciju sertifikata** (eng. *Certificate Distribution Systems - CDS*) i
- **PKI aplikacije.**

CP utvrđuje osnovne politike rada sertifikacionog tela i ostalih komponenti PKI sistema. Osnovne politike uključuju način objavljivanja zvaničnih dokumenata o sertifikaciji i lokaciji istih, načine identifikacije i autentifikacije korisnika, pisanje zahteva za izdavanje i povlačenje digitalnih sertifikata, tehničke zaštite i kontrole ovih zaštita, profil sertifikata, metode revizije i pravna pitanja.

CPS predstavlja dokument koji praktično opisuje rad sertifikacionog tela. U praksi, CPS predstavlja detaljnu razradu osnovnih politika sertifikacionog tela.

CA predstavlja osnovu poverenja i glavnu komponentu PKI sistema, sa osnovnim zadacima: generisanja digitalnih sertifikata, upravljanja životnim vekom sertifikata i osiguravanjem mehanizama povlačenja i ponovnog aktiviranja digitalnih sertifikata.

RA obezbeđuje interfejs između korisnika i CA, koji prihvata zahteve za izdavanje digitalnih sertifikata, proverava validnost ovih sertifikata, ali ih ne odobrava nego prosleđuje CA. Dakle RA ima ulogu predprocesora CA, sa značajnom ulogom provere identiteta korisnika.

CDS u praksi mogu biti rešeni na dva načina: direktno dostavljanje sertifikata korisnicima ili distribucija preko direktorijumskih servera.

PKI aplikacije obuhvataju softverska rešenja za: digitalno potpisivanje dokumenata, sigurnost web servera i email servera, sigurnost web transakcija, virtualne privatne mreže (*eng. Virtual Private Network – VPN*), sisteme za kontrolu pristupa i sl.

Elektronski potpis

Elektronski potpis se definiše kao skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i autentičnost potpisanog elektronskog dokumenta.

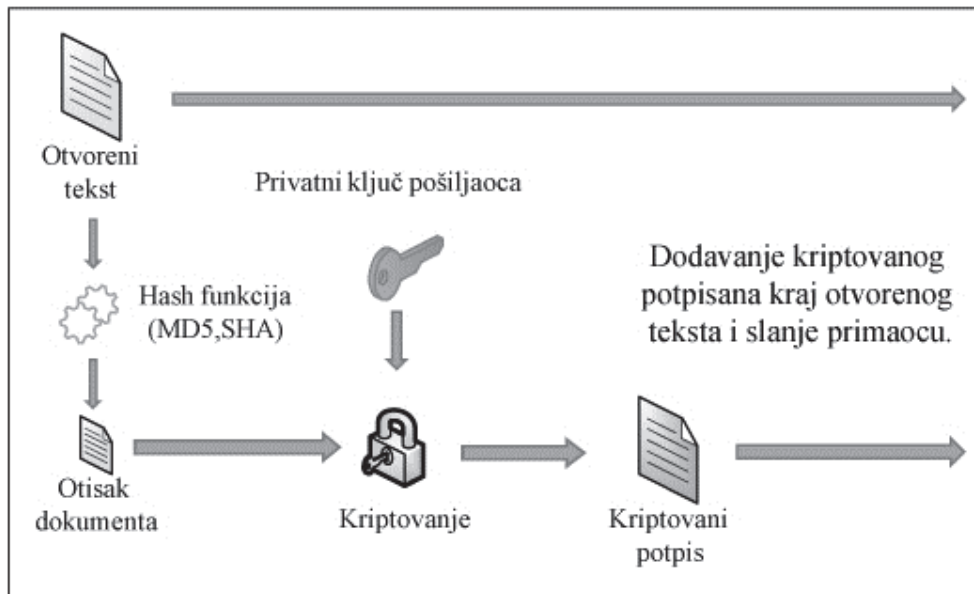
Takođe, **kvalifikovani elektronski potpis** definisan je kao elektronski potpis kojim se pouzdano garantuje identitet potpisnika i koji:

- je povezan isključivo sa potpisnikom,
- neosporno identifikuje potpisnika,
- nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika i
- direktno je povezan sa podacima na koje se odnosi i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka.

U praksi, elektronski potpis predstavlja postupak kojim se određeni blok podataka ili deo tog bloka kriptografski obeležava potpisnikovim tajnim parametrom. Kao što je već navedeno, svaki učesnik u PKI sistemu dobija svoj par ključeva: javni i privatni ključ. Javni ključ je dostupan svim učesnicima PKI sistema, a privatni ključ je poznat samo svom vlasniku. U slučaju kada privatni ključ postane poznat nekom drugom osim svog vlasnika, svi elektronski potpisi kreirani tim privatnim ključem su kompromitovani.

Postupak elektronskog potpisivanja dokumenta, prikazan na slici može se posmatrati kroz sledeće faze:

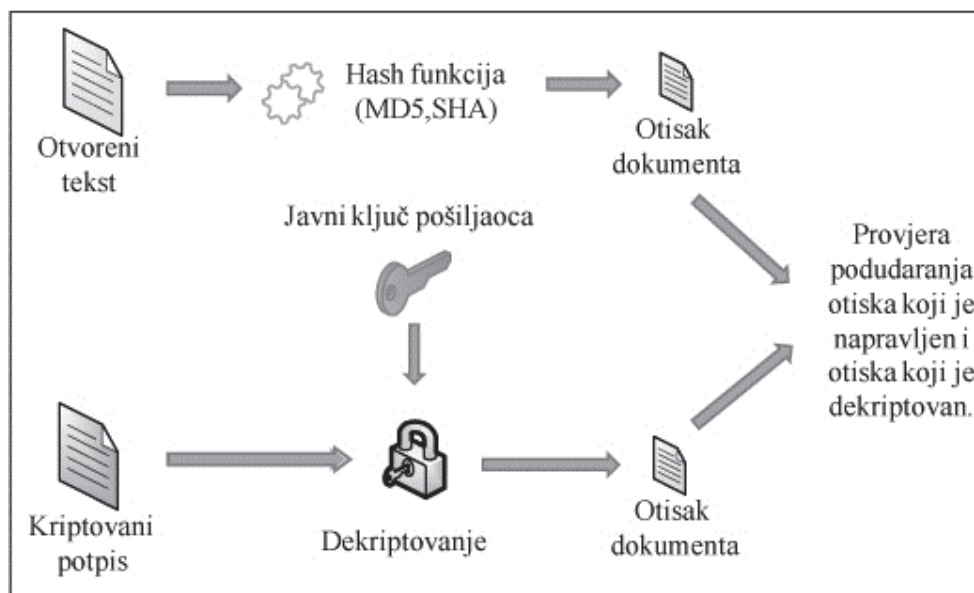
1. Prva faza podrazumeva primenu funkcija za kreiranje otiska, kao što su algoritam za kratak prikaz poruke (*eng. Message-Digest algorithm – MD*) ili sigurnosni hash standard (*eng. Secure Hash Standard – SHS*).
2. U drugoj fazi dobijeni otisak se šifrjuje tajnim ključem korisnika, primenom odgovarajućeg asimetričnog kriptografskog algoritma, kao što je RSA.
3. U trećoj fazi šifrovani otisak dodaje se na kraj originalne poruke i dobijeni blok podataka se šalje primaocu ili primaocima.



Slika 9: Kreiranje elektronskog potpisa

Postupak provere elektronskog potpisa, prikazan na slici može se posmatrati kroz sledeće faze:

- Prva faza podrazumeva prijem elektronski potpisanog dokumenta i razdvajanje originalne poruke od elektronskog potpisa.
- Druga faza je ponovna primena hash funkcije na originalni tekst. Ova funkcija mora odgovarati prvobitnoj hash funkciji koja se koristila prilikom elektronskog potpisivanja.
- Treća faza podrazumeva poređenje otiska koji smo dobili primenom hash funkcije i originalnog otiska. Ako su navedeni otisci identični tada je dokazana validnost elektronskog potpisa. U suprotnom, dokument se smatra kompromitovanim kao i privatni ključ pošiljaoca, tj. potpisnika dokumenta.



Slika 10: Provera elektronskog potpisa

Postoje mnoge kompanije koje nude gotova rešenja PKI sistema, jednostavna za implementaciju unutar neke institucije ili poslovnog procesa. Sigurnost ovih PKI sistema zavisi od algoritama i dužina ključeva koje se koriste za kriptovanje.

Direktive i standardi

Direktiva je pravni dokument Evropske Unije (EU) kojim se od zemalja članica zahteva određeni rezultat, bez davanja smernica kojima se dolazi do tog rezultata. Direktiva zahteva implementaciju, za razliku od regulative koja je samoizvršiva.

Osnovne direktive EU koje se odnose na PKI su:

- Direktiva 1999/93/EC Evropskog parlamenta i saveta i
- Odluka komiteta 2003/511/EC.

Direktiva 1999/93/EC ima za cilj olakšavanje upotrebe elektronskih potpisa kroz kreiranje potrebnih zakonskih okvira. Odluka komiteta 2003/511/EC nije obligatorna, već je predstavljena u vidu preporuka koje govore o sigurnosnim zahtevima elektronskih potpisa i proizvoda baziranih na njima. Konkretna lista standarda navedena je i grupisana po aneksima ove odluke.

Organizacija Internet Engineering Task Force (IETF) sastoji se od velikog broja radnih grupa koje rade na razvoju i promociji IKT standarda. Sve razvijene metode, zapažanja, preporuke, istraživanja i inovacije objavljuju

se u tzv. **zahtevima za komentarima** (eng. *Request for Comments – RFCs*).

Osnovni RFC dokumenti vezani za PKI su:

- RFC3820 - X.509 PKI, profil proxy sertifikata,
- RFC2560 - X.509 PKI, on-line protokol za prikaz statusa sertifikata (eng. Online Certificate Status Protocol – OCSP),
- RFC3647 - X.509 PKI, politike i uobičajene prakse sertifikacije,
- RFC2511 - X.509, format poruke za zahtev sertifikata,
- RFC2797 - poruke za upravljanje sertifikatima CMS,
- RFC3039 - X.509 PKI, profil kvalifikovanih sertifikata,
- RFC3161 - X.509 , PKI, Time-Stamp Protocol i
- RFC3281 - Profil atributa koji se koriste za autorizaciju sertifikata.

Internacionalna telekomunikaciona unija (eng. *International Telecommunication Union – ITU*) izdala je **ITU X.500**, preporuku za izgled baze podataka namenjene za globalnu upotrebu u vidu telefonskog imenika gde svaka organizacija upravlja svojim delom imenika. Ovakva globalna baza podataka je neophodna za postojanje globalnog PKI sistema unutar kog nema redundantnih podataka.

ITU X.509 je preporuka za strukturu elektronskih sertifikata. Prvi put je objavljena 1988. godine kao deo ITU X.500, nakon čega je sledila verzija 2 objavljena 1993. godine i verzija 3 objavljena 1996. godine, koja je trenutno aktivna.

X.500 nije šire prihvaćen u praksi, ali se X.509 ukorenio i sada je osnova za pružanje usluga digitalnih sertifikata.

Na osnovu X.509, na slici predstavljena je struktura digitalnog sertifikata.

Verzija obrasca x.509.
Serijski broj sertifikata
Jednoznačni identifikacioni kod
Algoritam kojim se vrši digitalni potpis (SHA1/RSA, MD5/RSA)
Naziv CA koje je izdalo sertifikat
Period važenja sertifikata
Vlasnik sertifikata, prema X.500
Podaci o javnom ključu potpisnika
Uslovi korišćenja sertifikata
Digitalni potpis sertifikata tajnim ključem sertifikacionog tela

Slika 11: Struktura digitalnog sertifikata

Sigurnost aktuelnih kriptografskih algoritama

Kako se sigurnost PKI sistema u celosti oslanja na sigurnost kriptografskih algoritama koji se koriste za kriptovanje/dekriptovanje u sastavu PKI, izuzetno je važno obezbediti i koristiti takve kriptografske algoritme koji obezbeđuju visok nivo sigurnosti. Do sada je osmišljeno na desetine kriptografskih algoritama koji su u upotrebi i koriste se u PKI sistemima koji obezbeđuju veoma dobru sigurnost i zaštitu visokog nivoa.

Na svetu postoji nekoliko naučno-istraživačkih grupa koje se bave procenama sigurnosti algoritama koje periodično daju preporuke dužina ključeva koji bi trebalo da su sigurni za korišćenje u periodu od narednih pet do osam godina. Jedna od takvih grupa je ECRYPT II koja radi po nalogu Evropske Komisije i redovno vrši analize i daje preporuke Evropskoj Komisiji o kriptografskim algoritmima i dužinama ključeva koje je sigurno koristiti. U godišnjem izveštaju za 2008.-2009.godinu, od 27. jula 2009. godine, grupa je dala preporuke za dužine ključeva.

Za procenu **minimalne dužine simetričnih ključeva** koristi se prilično jasan princip kojim se izračunava vreme potrebno za probijanje ključa napadom grubom silom ili pogađanjem kod kojih uspešnost probijanja zavisi isključivo od raspoložive procesne moći. Izračunavanje dužine ključa vrši se shodno raspoloživoj procesnoj snazi P i potrebnom vremenu štićenja podataka za koje se obično uzima životni vek zaštićenih podataka. Shodno tome, za minimalnu dužinu ključa uzima se n -bitna dužina takva da je $2n/P$ nešto duže od životnog vremena podataka (vremena štićenja podataka). Preporučene dužine ključeva po grupama napadača date su u tabeli:

Napadač	raspoloživi		Min. dužina	Vreme probijanja
	budžet	hardver		
"Haker"	0 usd	PC (s)	53	222 dana
	400 usd	FPGA	58	213 dana
Mala organizacija	10k usd	FPGA	64	278 dana
Srednje velika organizacija	300k usd	FPGA/ASIC	68	256 dana
Velika organizacija	10M usd	FPGA/ASIC	78	68 dana
Državna agencija	300M usd	ASIC	84	64 dana

Tabela 1: Preporučene dužine ključeva 2009.

Što se tiče procene **minimalnih „sigurnih“ dužina asimetričnih ključeva**, stvari su malo komplikovanije jer nepotrebno veliki ključevi mogu značajno da umanje performanse, postoji značajan i konstantno rastući broj napada koji su otkriveni u proteklih 30-ak godina, a koji daju rezultate

znatno brže i bolje od napada grubom silom te zbog pojave specijalnog kriptanalitičkog hardvera koji je znatno više od „naivnih“ mašina-pretraživača (eng. Search-Machines). Pored toga, simetričke i asimetrične sheme (algoritmi) se često koriste kombinovano – na primer asimetrični ključ se često koristi da se zaštiti simetrični.

Kako veća dužina ključeva značajno utiče na performance kriptovanja, značajno je proceniti koje dužine ključeva su dovoljne za obezbeđivanje kojeg nivoa sigurnosti podataka. Pojedine dužine ključeva dobro opremljene organizacije mogu da probiju u relativno kratkom periodu (reda veličine 60 – 90 dana). Zbog toga je i više nego zanimljivo napraviti pregled dužina simetričnih ključeva po procenjenim vremenima probijanja. Ovakva klasifikacija prikazana je u tabeli, gde * predstavlja nivo zaštite, a ** predstavlja minimalnu dužinu simetričnog ključa.

*	**	Nivo zaštite	Komentar
1.	32	Individualni napadi u realnom vremenu	Ne bi trebalo koristiti kod razvoja novih sistema
2.	64	Veoma kratkoročna zaštita protiv malih organizacija	
3.	72	Kratkoročna zaštita od srednje velikih organizacija i srednjoročna zaštita od malih organizacija	
4.	80	Veoma kratkoročna zaštita od agencija, dugoročna zaštita od malih organizacija	Najniži preporučeni nivo zaštite opšte namene koji obezbeđuje do 4 godine zaštite
5.	96	Standardni nivo zaštite	Preporučeni nivo zaštite opšte namene. Obezbeđuje zaštitu podataka u trajanju do oko 10 godina
6.	112	Srednjoročna zaštita	Obezbeđuje zaštitu podataka u trajanju do oko 20 godina
7.	128	Dugoročna zaštita	Dobar nivo zaštite i preporuka za zaštitu bitnih podataka. Obezbeđuje zaštitu podataka u trajanju do oko 30 godina
8.	256	Dugoročna zaštita u doglednoj budućnosti	Dobra zaštita od kvantnih računara

Tabela 2: Preporučene dužine ključeva po nivoima sigurnosti

III SOFTVERSKI PAKET “CASH TELEPORT”

1. Šta je softverski paket “Cash Teleport”

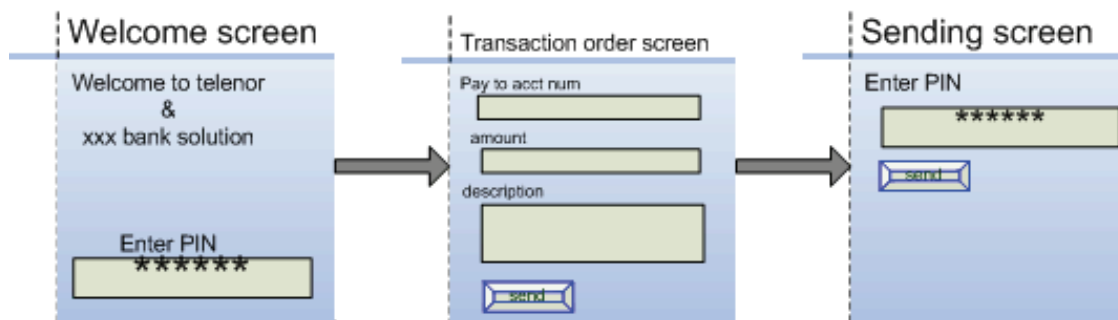
"Cash Teleport" je matematičko rešenje za šifrovanje i dešifrovanje SMS i DATA poruka.

Dizajniran je za potrebe banaka i drugih finansijskih institucija koje zahtevaju najveći stepen bezbednosti podataka njihovih klijenata i svakodnevnih transakcija novca.

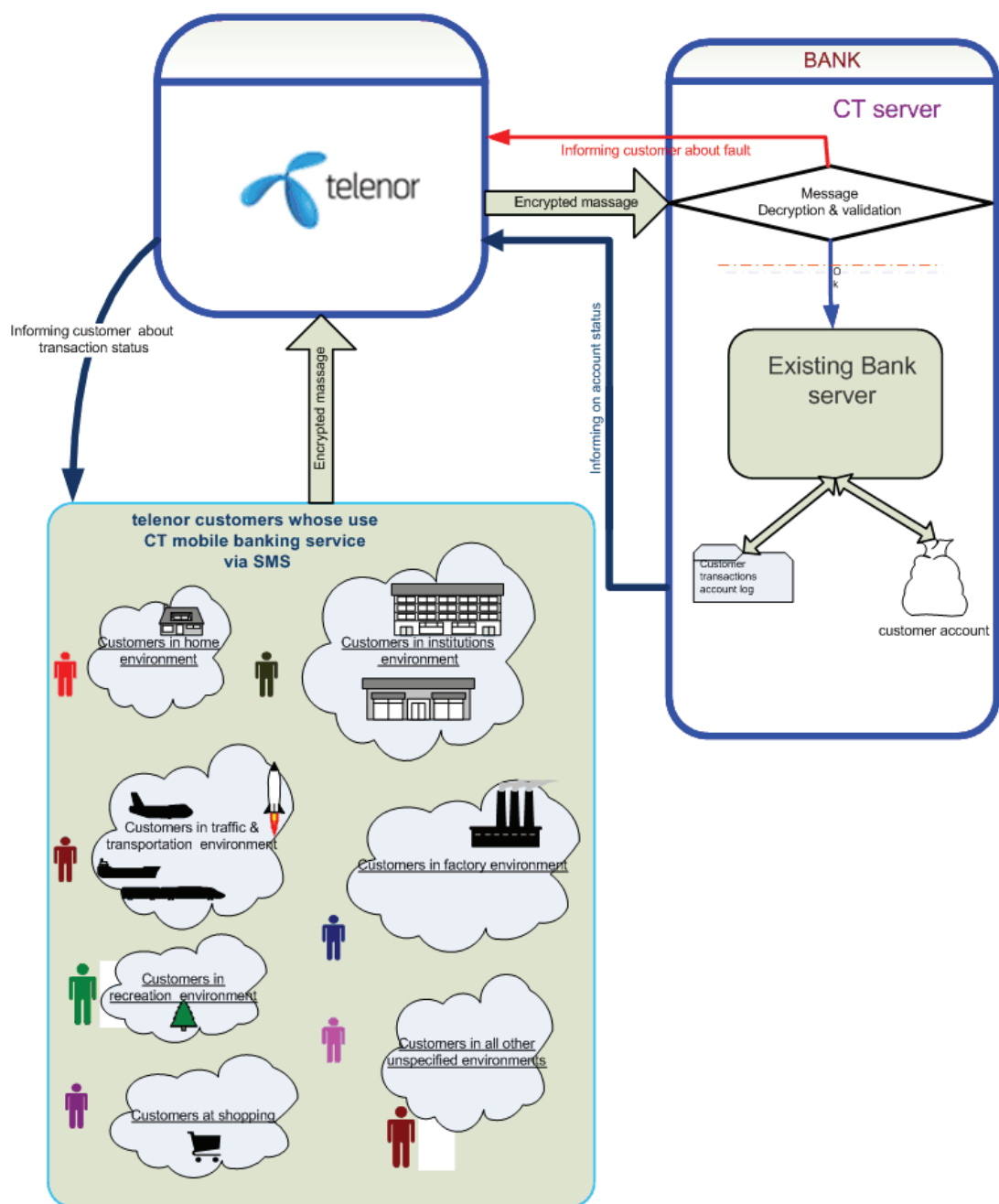
Omogućava zaštićenu komunikaciju između banke i njenih klijenata. Poruke poslate preko CashTeleport softvera ne mogu se neovlašćeno dešifrovati. Premašuje najviše bezbednosne zahteve.

Omogućava visok nivo autentikacije, tajnosti, neporecivosti i integriteta poruka

Primenom u **Mobilnom bankarstvu**, korisnicima bi bilo omogućeno da putem SMS-a izdaju nalog banci da sredstva sa svog postojećeg računa prebace na neki drugi račun tj. da se izvrši plaćanje. Koristeći ovu uslugu korisnici će jednostavnije, brže i bezbednije moći da manipulišu svojim sredstvima *na bankarskim računima*. Konkretno, koristeći ovo rešenje moći će da izvrše plaćanja sa bilo kog mesta u bilo koje vreme isto kao da se u tom momentu nalaze *na šalteru* u banci ali bez ličnog dolaska, bez čekanja u redovima, bez ograničenja radnog vremena, nepotrebnog stresa, koristeći samo svoj mobilni telefon (bez posebne operme), lako, brzo i bezbedno.



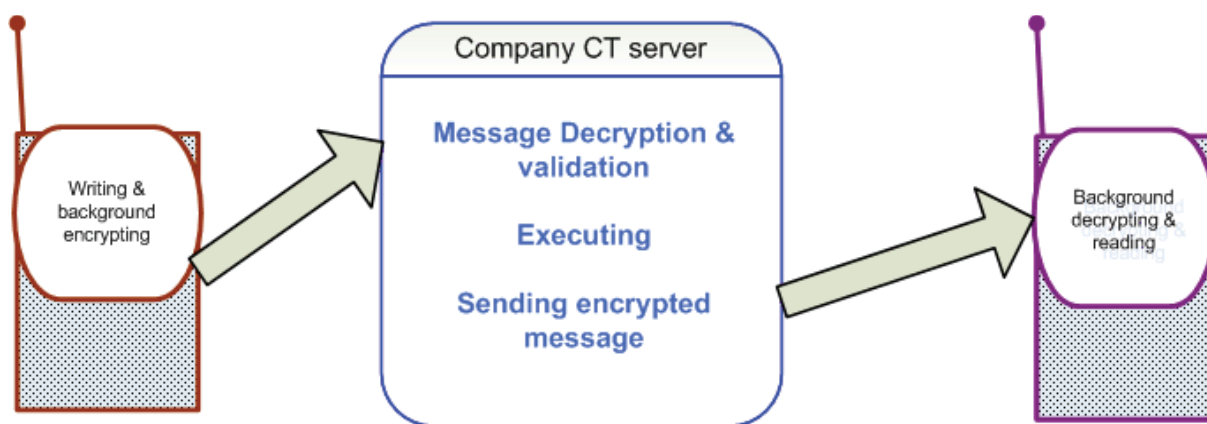
Slika 12: izgled klijentske aplikacije



Slika 13: slika svih učesnika u lancu mobilnog bankarstva

Šifrovana komunikacija:

Primenom Cash Teleport rešenja omogućava se šifrovanje SMS poruka koje ispunjavaju uslove autentikacije, tajnosti, integriteta i neporecivosti . Usluga šifrovane komunikacije je predviđena za velike organizacione celine (velike kompanije i državne ustanove – mup , vojska, vlada...) koje imaju potrebu da njihovi zaposleni međusobno često razmenjuju poverljive poslovne podatke. CT system upravo to omogućava. Korišćenjem CT načina šifrovanja moguće je poslati SMS poruku za koju možete biti siurni da je može pročitati samo onaj kome je poslata. Za primljenu poruku putem ovog sistema možete biti sigurni daje pošiljaoc upravo onaj za koga se predstavlja kao i da tekst poruke upravo onaj koji je on poslao. Tekst poruke nije moguće neovlašćeno pročitati ni modifikovati.



Slika 14: prikaz komunikacije između dva klijenta

2. Način rada

- Banka svojim zainteresovanim klijentima vrši instalaciju aplikacije za MBanking na mobilni telefon (vreme instalacije oko 5 minuta)
- Svaki klijent dobija jedinstvene enkripcijske ključeve
- Klijent vrši plaćanje putem aplikacije na mobilnom telefonu unošenjem parametara za prenos sredstava
- Nakon serverske validacije poruke server vrši prenos sredstava i putem SMS obaveštava učesnike

3. Tehnička implementacija

- CashTeleport se lako povezuje sa već postojećim informacionim sistemom banke i fizički se nalazi u banci
- Period implementacije u postojeći sistem banke je veoma kratak
- Ne iziskuje značajnija ulaganja u opremu
- Lak je za redovno održavanje i potpuno automatizovan
- Samo banka raspolaže ključevima i ima potpunu kontrolu svih podataka

4. Prednosti Softverski paket "Cash Teleport"

Prednosti za banku

- Nova usluga koja donosi konkurentsku prednost
- Povećanje broja transakcija po klijentu
- Povećanje broja klijenata
- Povećanje zadovoljstva klijenata
- Smanjenje rizika u poslovanju
- Smanjenje troškova

Prednosti za klijente

- Bezbedan i praktičan način plaćanja u realnom vremenu
- Moguće plaćanje sa bilo koje lokacije pokrivene GSM signalom
- Minimalna mogućnost zloupotrebe
- Ne iziskuje dodatne troškove, koristi se na postojećem mobilnom telefonu
- Izvestaj o izvršenom plaćanju momentalno dostupan u elektronskom obliku
- Mogućnost slanja sredstava na bilo koji bankomat u mreži

Konkurentske prednosti

- CashTeleport je potpuno nov algoritam za enkripciju,
- 1064 bitna enkripcija,
- Kompatibilan na svim GSM mrežama,
- Funkcionalan na skoro svim modelima mobilnih telefona,
- Ne koristi Internet,
- Nema treće strane od poverenja.

5. Potencijalni korisnici ove usluge su:

- Državne institucije (mup, vojska, vlada, sva ministarstva),
- Velike kompanije,
- Mala i srednja preduzeća.

Takođe, ovu uslugu mogu koristiti i grupe fizičkih lica koje nisu u okviru jedne organizacione celine. Te grupe se po potrebi mogu firmirati i modifikovati.

Suština CT sistema je u matematičkim algoritmima koji omogućavaju kvalitetno šifrovanje.

6. Kriterijumi bezbednosti

CashTeleport ispunjava sve osnovne kriterijume bezbednosti podataka:

- **Privatnost** – neovlašćena lica neće biti u mogućnosti da dešifruju tekst poruke čak ni korišćenjem svih do danas poznatih alata.
- **Autentikacija** – sa sigurnošću možemo prihvatiti da je pošiljaoc poruke upravo onaj za koga se predstavlja.
- **Neporecivost** – pošiljaoc validnog naloga ne može poreći da je primljeni nalog identičan poslatom.
- **Integritet** – tekst primljenog naloga u potpunosti odgovara tekstu poslatog naloga. Svaka promena teksta se automatski prepoznaje.

Kvalitet ovog algoritma je potvrđen od strane Matematičkog Instituta Srpske Akademije Nauka i Umetnosti koja je najmerodavnija institucija ovog tipa u Srbiji.

IV EVALUACIJE KRIPTOGRAFSKE SIGURNOSTI "CASH TELEPORT"

Evaluaciju kriptografske sigurnosti "Cash Teleport" izvršio je Matematički institut SANU iz Beograda i dao IZJAVU o evaluaciji kriptografske sigurnosti "Cash Teleport" kriptografskog modela – faksimil na strani 7.

1. Polazišta evaluacije kriptografske sigurnosti "Cash Teleport"

Evaluacija kriptografske sigurnosti "Cash Teleport" polazi od sledećeg:

1. Model SMS koje se razmatra je sledeći:
 - SMS je binarni vektor dužine $160 \times 7 \times 8 = 8960$ bita;
 - prvih 4024 (4212) - 4480 bita se mogu koristiti kao podrška za ostvarivanje bezbednosti preostalih 4480 - 4936 bita koji se označavaju kao poruka;
 - nema drugih ograničenja vezanih za strukturu SMS-a.
2. Zastita poruke podrazumeva sledeće:
 - autentifikaciju podataka;
 - zaštitu tajnosti podataka.
3. Za kontrolu autentičnosti poruka koristiti kriptografsku tehniku Message Authentication Code (MAC).
4. Za zaštitu tajnosti primeniti sekvencijalno šifrovanje sa niskim ukupnim dodatnim opterećenjem na celinu "Cash Teleport".
5. Težiti minimizaciji dimenzije softvera neophodnog za funkcionisanje "Cash Teleport" na klijentskoj strani.
6. Koristiti kriptografske ključeve ukupne dužine približne zbiru dužina binarnih Password 1 i Password 2 iz inicijalnog "Cash Teleport" resenja.
7. Koristiti parametar "vreme" podrazumevajući da je raspoloživ u formi I-dimenzionalnog binarnog vektora, gde je I promenljiva veličina čija se partikularna vrednost specificira saglasno željenom nivou sigurnosti i implementacionim ograničenjima.

2. Opšta paradigma zaštite poruka

Zaštita poruka koja je predmet razmatranja obuhvata kontrolu autentičnosti poruka i zaštitu tajnosti poruka, primenom tehnika zasnovanih isključivo na tajnim kriptografskim ključevima.

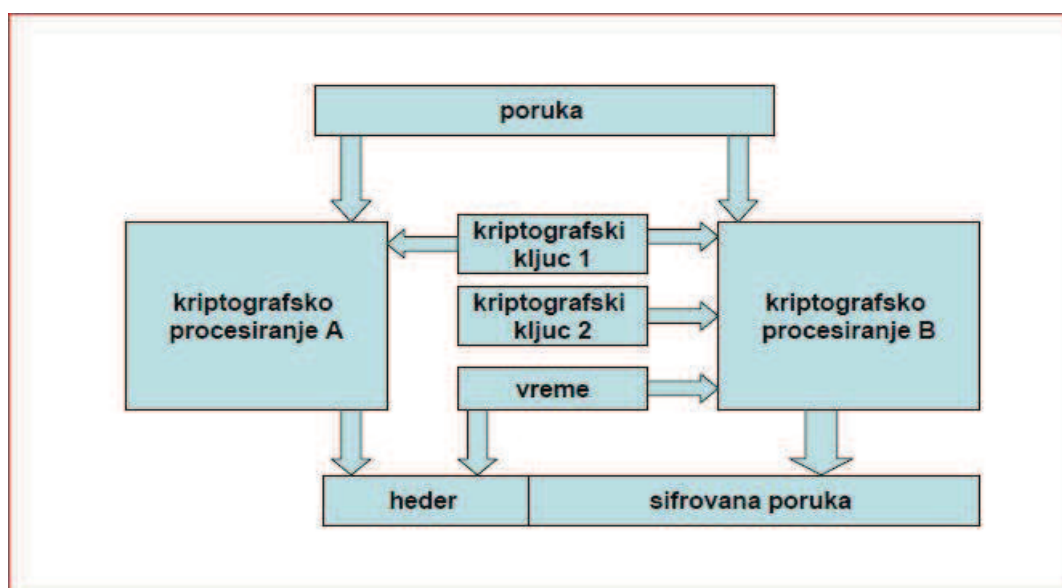
3. Kriptografski ključevi

Kriptografski ključevi koji se koriste u sistemu obuhvataju:

- kriptografske ključeve kod svakog klijenta;
- kriptografske ključeve na serverskoj strani.

Podrazumeva se da različiti klijenti imaju različite kriptografske ključeve i da server poseduje ključeve svakog od klijenata i da na osnovu poznavanja identiteta klijenata jednoznačno identifikuje kriptografske ključeve klijenta.

Pretpostavka je da svaki klijent poseduje sledeća dva kriptografska ključa (koji korespondiraju parovima Password 1 i Password 2):



Slika 15: procesiranje na klijentskoj strani

- Kriptografski ključ 1 u formi binarnog niza dužine $L1$;
- Kriptografski ključ 2 u formi binarnog niza dužine $L2$ za konstantu veće od dužine binarne reprezentacije poruke.

Podrazumeva se da su dužine $L1$ i $L2$ izabrane tako da su u saglasnosti sa:

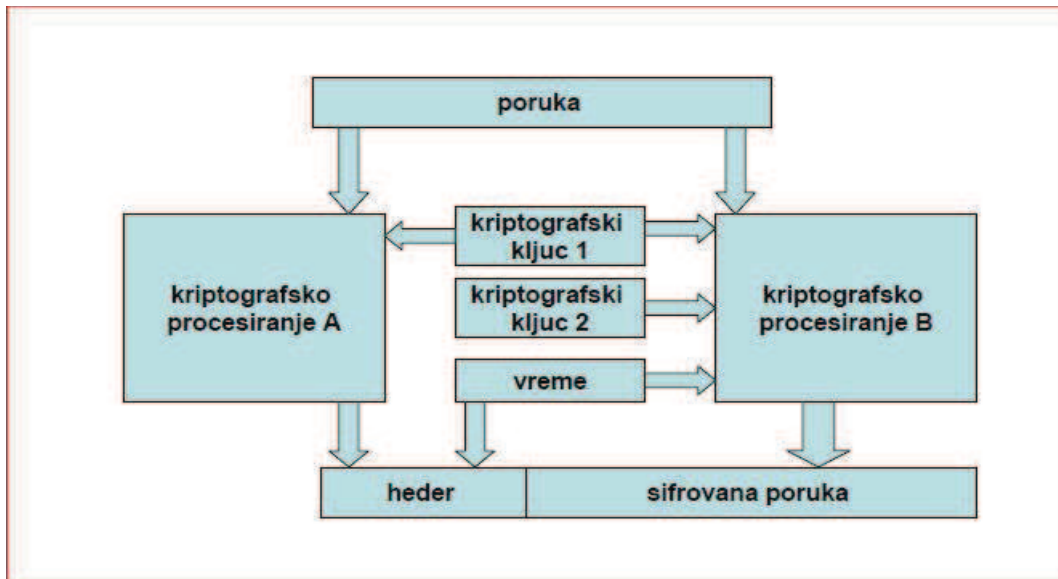
- konkretnom selekcijom primenjenih kriptografskih primitiva;
- željenim nivoom kriptografske sigurnosti; i
- implementacionim ograničenjima.

4. Procesiranje na klijentskoj strani

Generički izgled šeme procesiranja na klijentskoj, predajnoj strani, radi ostvarivanja kontrole autentičnosti i zaštite tajnosti "Cash Teleport" poruka je prikazan na slici.

5. Procesiranje na serverskoj strani

Generički izgled šeme procesiranja na serverskoj, prijemnoj strani, radi ostvarivanja kontrole autentičnosti i zaštite tajnosti "Cash Teleport" poruka je prikazan na slici.

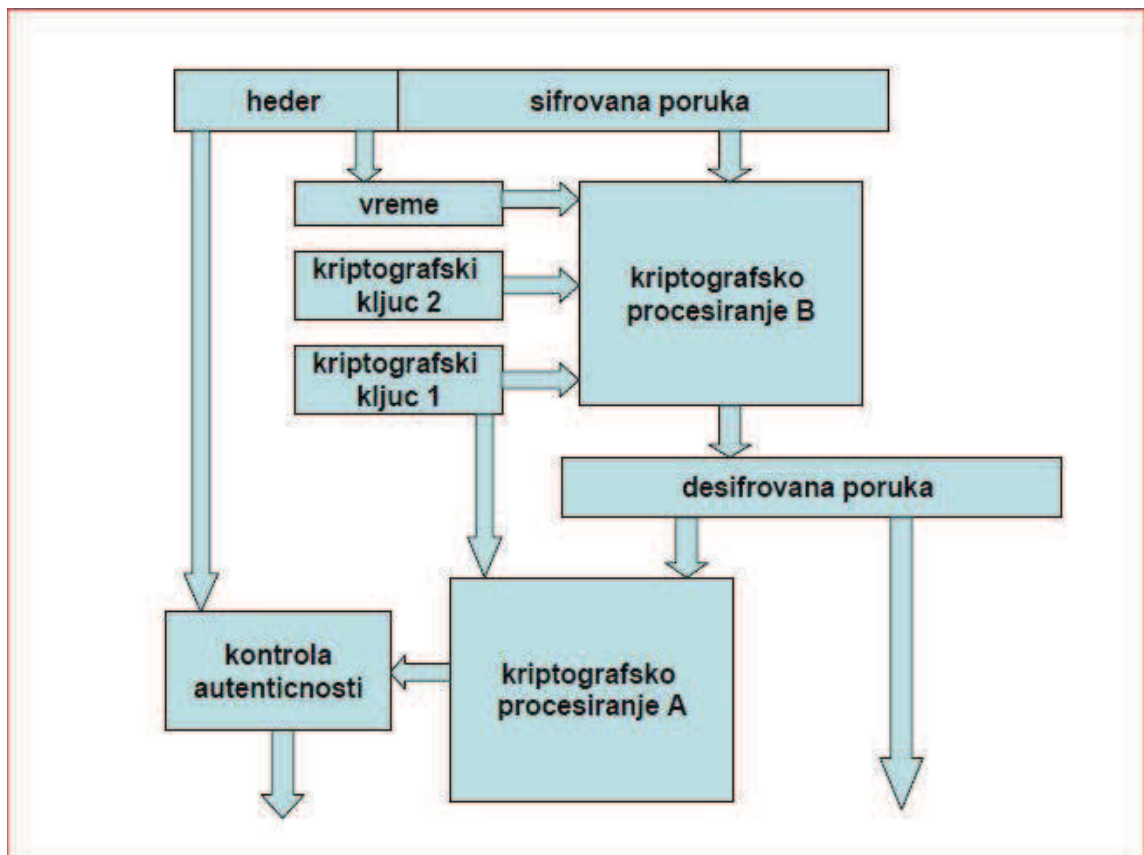


Slika 16: Osnovna šema procesiranja na serverskoj – predajnoj strani

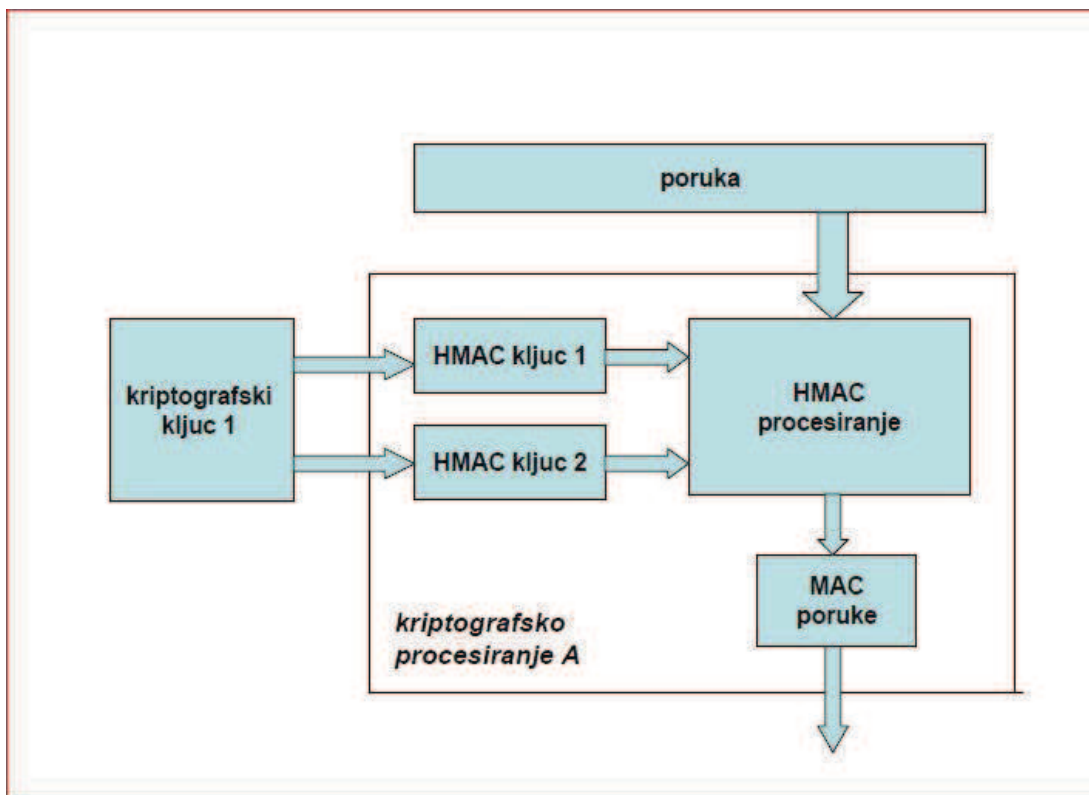
Kriptografsko procesiranje A

Kriptografskim procesiranjem A obezbeđuje se kontrola autentienosti poruka.

a) Generički okvir



Slika 17: Predlog generičke šeme kriptografskog procesiranja A za ostvarivanje kontrole autentičnosti.



Slika 18 : Generičeka šema kriptografskog procesiranja A za ostvarivanje kontrole autentičnosti

Predložena generička sema pretpostavlja primenu HMAC algoritma saglasno [27].

b) Partikularna forma

Generička šema za kriptografsko procesiranje A obuhvata familiju partikularnih algoritama koji su determinisani sledećim:

- Selekcijom partikularne Hash funkcije;
- Selekcijom parametara algoritma.

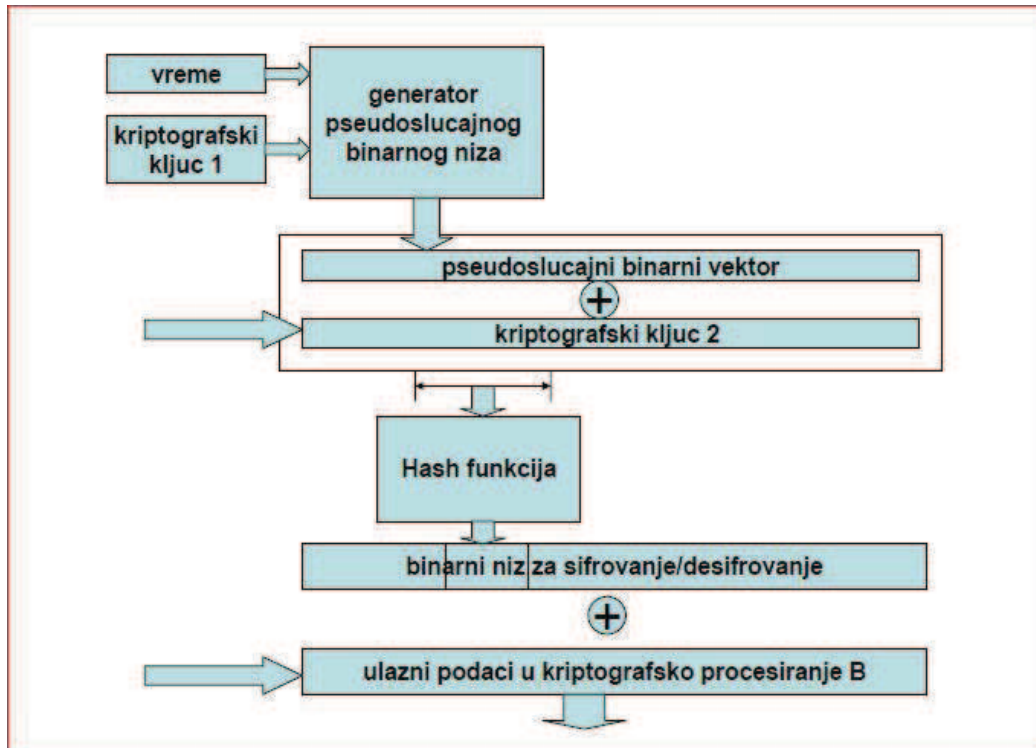
Kao partikularni preporučljiv izbor za Hash funkciju predlaže se SHA-1, [26].

6. Kriptografsko procesiranje B

Kriptografskim procesiranjem B ostvaruje se zaštita tajnosti poruka tokom prenosa javnim radio kanalom kroz šifrovanje poruka na klijentskoj (predajnoj) strani i dešifrovanje na serverskoj (prijemnoj) strani.

a) Generički okvir

Predlog generičke šeme kriptografskog procesiranja B za ostvarivanje zaštite tajnosti prikazan je na slici.



Slika 19: Generička šema kriptografskog procesiranja B za ostvarivanje zaštite tajnosti.

Algoritam za kriptografsko procesiranje B kao osnovne komponente uključuje:

- generator pseudoslučajnog binarnog niza,
- hash funkciju.

Binarni niz za šifrovanje/dešifrovanje generiše se saglasno sledećim osnovnim koracima.

- 1) Na osnovu vektora "vreme" i "kriptografski ključ 1" vrši se inicijalizacija generatora pseudoslučajnog binarnog niza.

- 2) Polazeći iz formiranog inicijalnog stanja, generator proizvodi binarni pseudoslučajni vektor.

Preporučuje se da posle inicijalizacije, a pre generisanja binarnog pseudoslučajnog vektora generator napravi N "okreta" koji se ne koriste, gde je N parametar čija vrednost zavisi od željenog nivoa kriptografske sigurnosti i implementacionih ograničenja.

- 3) Generisani pseudoslučajni binarni vektor se bit-po-bit sabira po modulu 2 sa Kriptograskim ključem 2. Segmenti rezultujućeg vektora se mapiraju pomoću Hash funkeije saglasno sledećem.

- Neka su $\mathbf{A}$, L_{block} i L_{hash} određeni parametri kriptografskog procesiranja B.
- Hash funkeija sa slike vrši hash preslikavanje preklapajućih segmente dužine L_{block} zbirnog binarnog vektora u binarne segmente dužine L_{hash} ;
- Segmenati koji se mapiraju Hash funkcijom dobijaju se pomeranjem L_{block} -dimenzionalnog prozora sa korakom $\mathbf{A}$;

- 4) Binarni niz za šifrovanje/dešifrovanje se formira konkatencijom (nadovezivanjem) $L/jas/j$ -dimenzionalnih hash vrednosti.

Šifrovanje/dešifrovanje ulaznog binarnog vektora u algoritam za kriptografsko procesiranje B se realizuje bit-po-bit sabiranjem po modulu 2 ulaznog vektora i generisanog vektora za šifrovanje/dešifrovanje.

b) Partikularna forma

Generička šema za kriptografsko procesiranje B obuhvata familiju partikularnih algoritama koji su determinisani sledećim:

- Selekcijom partikularnog generatora pseudoslučajnog binarnog niza i tehnike njegove inicijalizacije na osnovu vektora "vreme" i "kriptografski ključ 1";
- Selekcijom partikularne Hash funkcije;
- Selekcijom parametara algoritma.

Kao partikularni mogući izbor za generator pseudoslučajnog binarnog niza predlaže se "Self-Shrinking Generator" specificiran saglasno opisu i za dizajn relevantnim rezultatima njegove evaluacije kriptografske sigurnosti prikazanim u [28] i [29].

Kao partikularni preporučljiv izbor za Hash funkciju predlaže se SHA-1, [26].

7. Zaključna diskusija kriptografske evaluacije

Predložen je generički okvir koji definise familiju mogućih tehnika za kontrolu autentičnosti i zaštitu tajnosti poruka.

Predloženi okvir omogućuje fleksibilnost selekcije:

- primerenog nivoa kriptografske sigurnosti;
- primerenog nivoa implementacionog opterećenja celine sistema u koji se "Cash Teleport" ugrađuje;
- primerenog nivoa radnog opterećenja celine sistema u koji se "Cash Teleport" ugrađuje.

Napominje se da je najčešće kritično implementaciono i radno opterećenje klijentske strane.

Nivo kriptografske sigurnosti partikularnih varijanti suštinski zavisi od selektovanih komponenti i setovanja parametara "Cash Teleport" kriptografskog rešenja.

V ZAKLJUČAK

Očekuje se da mobilno bankarstvo, u nekom svom obliku, polako zamenjuje platne kartice u celom svetu. Na tom svom putu će se susresti sa velikim izazovima u čije prevazilaženje će biti investirano i nekoliko desetina milijardi dolara. Jedan od glavnih izazova je upravo bezbednost transakcija. Ukoliko bezbednosni izazov ne bude prevaziđen mobilno bankarstvo nikada neće dostići očekivane razmere. Ni platne kartice koje su sada dominantan način plaćanja nemaju idealno rešen bezbednosni problem ali ipak su uspele da zažive i donekle zamene „keš“ plaćanja. Nažalost, nikada nećemo znati koji bi zapravo bili kapaciteti platnih kartica i kojom brzinom bi one osvojile tržišta jer su upravo zbog bezbednosnih rizika mnogi korisnici odustali od korišćenja platnih kartica (ili izvršavanja konkretnih transakcija). Takođe, tajni je podatak koliko su banke i osiguravajuće kuće platile zbog raznih bezbednosnih propusta.

Problem bezbednosti mobilnog bankarstva u postojećim modelima pokušava da se prevaziđe savremenom opremom (mobilnim telefonima jake procesorske snage), kvalitetnim vezama (velika brzina i dobra pokrivenost internetom) kao i komplikovanim procedurama. To ima za direktnu posledicu smanjenje veličine tržišta ograničavajući se na one koji imaju novca da kupe savremene mobilne telefone, one koji su dovoljno edukovani da koriste nove alate i one koji žive na mestima koja su pokrivena kvalitetnim signalom. Takođe, i sa tim preduslovima, funkcionalnosti mobilnog bankarstva još nisu na nivou platnih kartica. Ne postoji mogućnost plaćanja u realnom vremenu, podizanja novca sa bankomata, obavljanje transakcija za par sekundi itd. Funkcionalnost i lakoća korišćenja su odlučujući faktor kada se neka usluga ili proizvod plasira na tržište. Po sadašnjim istraživanjima tržišta, na ponuđenim rešenjima, je potrebno još dosta da se radi.

U prošlosti, u sadašnjosti i u budućnosti, bezbednost komunikacija se štiti šifarskim algoritmima. Razvojem matematike i informatike neki od algoritama su se pokazali prihvatljivim, dok su brojni pokazali slabosti na specifične tipove napada. Te slabosti su uticale da se neki algoritmi izmene a neki da prestanu da se koriste. Proizvodi koji su ih koristili uglavnom su povučeni sa tržišta ili zamenjeni.

Problem bezbednosti podataka u protoku ne tiče se samo mobilnog bankarstva već se prožima kroz sve savremene poslovne procese. Mi živimo u informatičkom društvu. Informatičko se zove baš zbog vrednosti informacija u svakodnevnom životu i poslovanju. Svakom danom vrednost tih informacija postaje sve veća. Vrlo mali procenat ljudi koristi neki vid

zaštite svojih komunikacija. Osnovni razlog za to je nesvesnost rizika i nedostupnost adekvatnih alata.

U ovom radu je predstavljeno autorsko rešenje za šifrovanje podataka "**Cash teleport**". On može da prevaziđe sve glavne prepreke savremenog mobilnog bankarstva. Napravljen je tako, da je moguće izvršiti šifrovanje SMS poruke a da pritom budu ispunjeni svi bezbednosni atributi.

- Autentikacija - možemo biti sigurni da je pošiljaoc zaista onaj za koga se predstavlja,
- Tajnost - poruku ne može otvoriti/dešifrovati neovlašćeno lice,
- Integritet - tekst poruke je upravo onaj koji je poslat,
- Neporecivost - pošiljaoc validne poruke ne može poreći da je baš on, baš tu poruku poslao.

U ovom rešenju **nema** "treće strane od poverenja" što je prava retkost u postojećim alatima za bezbednost podataka u protoku.

Internet nije preduslov korišćenja **Cash Telporta**. Baš iz tog razloga fizički je onemogućen hakerski napad preko tog kanala. Ali ovi algoritmi mogu vršiti i šifrovanje podataka koji mogu biti poslani preko Interneta.

Za šifrovanje koristi: i simetrične i hash algoritme, koji se u slučaju naučnog prevazilaženja određenog algoritma mogu lako izmeniti.

Takođe dužine ključeva se mogu prilagođavati zakonskim i klijentskim zahtevima i preduslovima.

Cash Teleport može raditi na skoro svim mobilnim telefonima koji su prisutni na tržištu i ne zahteva dodatni hardver. Takođe, ne ometa ostale funkcije telefona.

Cash Teleport se može koristiti za potrebe mobilnog bankarstva ali i za mnoge druge potrebe kao što su:

- Šifrovana SMS komunikacija,
- Šifrovana komunikacija glasom,
- Izdavanje naloga mašinama (M2M),
- Mobilno klađenje,
- Internet plaćanja,
- Autentikacija na Internet sajtove,

VI LITERATURA

- [1] A.J. Menezes, P.C. van Oorschot and S.A. **Vanstone**, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997.
- [2] *Handbook of Information Security*, H. Bidgoli, Editor-in-Chief, vols. 1-3. John Wiley & Sons, Hoboken, New Jersey, 2006. (ISBN: 0-471-648333-7)
- [3] M. Bellare, "New Proofs for NMAC and HMAC: Security without Collision-Resistance", CRYPTO 2006, *Lecture Notes in Computer Science*, vol. 4117, Aug. 2006.
- [4] **M.** Bellare, R. Canetti and H. Krawczyk, "Keying Hash Functions for Message Authentication", CRYPTO '96, *Lecture Notes in Computer Science*, vol. 1109, pp. 1-15. 1996.
- [5] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, and W. Jalby "Collisions of SHA-0 and Reduced SHA-1", EUROCRYPT 2005, *Lecture Notes in Computer Science*, vol. 3494, pp. 36-57, May 2005.
- [6] S. Contini and Y. Lisa Yin, "Forgery and Partial Key Recovery Attacks on HMAC and NMAC Using Hash Collisions", ASIACRYPT 2006, *Lecture Notes in Computer Science*, vol. 4284, pp. 37-53, Dec. 2006; extended version available at IACR, Cryptology ePrint Archive, Report 2006/319, Sept. 2006, 21 pages, <http://eprint.iacr.org/2006/319.pdf>.
- [7] S. Halevi and H. Krawczyk, "Strengthening Digital Signatures Via Randomized Hashing", CRYPTO 2006, *Lecture Notes in Computer Science*, vol. 4117, pp. 41-59, Aug. 2006.
- [8] J. Kim, A. Biryukov, B. Preneel and S. Hong, "On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1", IACR, Cryptology ePrint Archive, Report 2006/187, Aug. 2006, 11 pages, <http://eprint.iacr.org/2006/187.pdf>.
- [9] NIST's Policy on Hash Functions, 2006. available online at <http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NISTPolicyonHashFunctions.htm>.
- [10] C. Rechberger and V. Rijmen, "Note on Distinguishing, Forgery, and Second Preimage Attacks on HMAC-SHA-1 and a Method to Reduce the Key Entropy of NMAC", IACR, Cryptology

ePrint Archive, Report 2006/290, Aug. 2006, 11 pages,
<http://eprint.iacr.org/2006/290.pdf>.

- [11] RSA Security, www.rsa.com
- [12] M. Stevens, A. Lenstra and B. de Weger, "Target Collisions for MD5 and Colliding X.509 Certificates for Different Identities version", IACR, Cryptology ePrint Archive, Report 2006/360, Nov. 2006, 15 pages, <http://eprint.iacr.org/2006/360.pdf>
- [13] X. Wang and H. **Yu**, "How to Break **MD5** and Other Hash Functions", **EUROCRYPT** 2005, *Lecture Notes in Computer Science*, **vol.** 3494, pp. 1935, May 2005.
- [14] X.Y. Wang. H.B. Yu, Y. Lisa Yin, "Efficient Collision Search Attacks on SHA-0", CRYPTO 2005, *Lecture Notes in Computer Science*, **vol.** 3621, pp. 1-16, Aug. 2005
- [15] X. Wang, Y. L. Yin and H. Yu, "Finding Collisions in the Full SHA-1", CRYPTO 2005, *Lecture Notes in Computer Science*, **vol.** 3621, pp. 17-36, Aug. 2005.
- [16] E. Barkan, E. Biham and A. Shamir, "Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs", CRYPTO 2006, *Lecture Notes in Computer Science*, **vol.** 4117, pp. 1-21, Aug. 2006.
- [17] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers", ASIACRYPT 2000, *Lecture Notes in Computer Science*, **vol.** 1976, pp. 1-13, 2000.
- [18] A. Biryukov, S. Mukhopadhyay and P. Sarkar, "Improved Time-Memory **Trade-Offs** with Multiple Data", SAC 2005, *Lecture Notes in Computer Science*, **vol.** 3897, pp. 110-127, June 2006.
- [19] A. Fiat and **M.** Naor, "Rigorous time/space trade-offs for inverting functions", *SIAM J. Computing*, **vol.** 29, pp. 790-803, 1999.
- [20] M.E. Hellman, "A cryptanalytic time-memory trade-off", *IEEE Trans. Inform. Theory*, **vol.** IT-26, pp. 401-406, July 1980.
- [21] J. Hong and P. Sarkar, "New Applications of Time Memory Data Tradeoffs", ASIACRYPT 2005, *Lecture Notes in Computer Science*, **vol.** 3788, pp. 359-372, Dec. 2005.

- [22] J.J. Hoch and A. Shamir, "Fault Analysis of Stream Ciphers", CHES 2004, *Lecture Notes in Computer Science*, **vol.** 3156, pp. 240-253, 2004.
- [23] M.J. Mihaljevic, M.P.C. Fossorier and H. Imai, "Security Weaknesses of Certain Broadcast Encryption Schemes", *Lecture Notes in Computer Science*, **vol.** 3919, pp. 228-245, July 2006.
- [24] M.J. Mihaljevic, M.P.C. Fossorier and H. Imai, "A General Formulation of Algebraic and Fast Correlation Attacks Based on Dedicated Sample Decimation", *Lecture Notes in Computer Science*, vol. 3857, pp. 203-214, Feb. 2006.
- [25] M.P.C. Fossorier, M.J. Mihaljevic, H. Imai, Y. Cui and K. Matsuura, "An Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocols for RFID Authentication", *Lecture Notes in Computer Science*, vol. 4329, pp. 48-62, Dec. 2006.
- [26] SHA-1: FIPS PUB 180-1, Federal Information Processing Standards Publication 180-1, 1995.
- [27] RFC 2104, HMAC: Keyed-Hashing for Message Authentication.
- [28] M. Hell and T. Johansson , "Two New Attacks on the Self-Shrinking Generator", *IEEE Trans. Inform. Theory*, **vol.** 52, pp. 3837-3843, August 2006.
- [29] B. Zhang and D. Feng, "New Guess-and-Determine Attack on Self-Shrinking Generator", *Lecture Notes in Computer Science*, vol. 4284, pp. 54-68, Dec. 2006.

Sadržaj slika i tabela

Slika 1: Prijava autorskog dela Cash teleport	4
Slika 2: Prijava autorskog dela Koncept bezbedne transakcije.....	5
Slika 3: Potvrda MI SANU.....	6
Slika 4: POS i POS touchscreen	30
Slika 5: Izgled bankomata	32
Slika 6: Aplikacija u mobilnom bankarstvu	45
Slika 7 : Princip rada simetričnog kriptografskog sistema	49
Slika 8: Princip rada asimetričnog kriptografskog sistema	50
Slika 9: Kreiranje elektronskog potpisa.....	53
Slika 10: Provera elektronskog potpisa.....	54
Slika 11: Struktura digitalnog sertifikata.....	55
Tabela 1: Preporučene dužine ključeva 2009.....	56
Tabela 2: Preporučene dužine ključeva po nivoima sigurnosti	57
Slika 12: Izgled klijentske aplikacije	58
Slika 13: Slika svih učesnika u lancu mobilnog bankarstva.....	59
Slika 14: Prikaz komunikacije između dva klijenta.....	60
Slika 15: Procesiranje na klijentskoj strani	64
Slika 16: Osnovna šema procesiranja na serverskoj – predajnoj strani	65
Slika 17: Predlog generičke šeme kriptografskog procesiranja A za ostvarivanje kontrole autentičnosti.	66
Slika 18 : Generička šema kriptografskog procesiranja A za ostvarivanje kontrole autentičnosti	67
Slika 19: Generička šema kriptografskog procesiranja B za ostvarivanje zaštite tajnosti.....	68