

УНИВЕРЗИТЕТ СИНГИДУМУ
ПОСЛОВНИ ФАКУЛТЕТ

ДИПЛОМСКИ РАД

ЕЛЕКТРОНСКИ КАНАЛИ БАНКАРСКОГ ПОСЛОВАЊА

Ментор:
Доц. др Марко Шарац

Студент:
Марко Дервишевић 103982/2009

Београд, 2014.

САДРЖАЈ

УВОД.....	3
1. РЕАЛНИ НОВАЦ У СУБЕР ПРОСТОРУ.....	4
1.1. Како настаје електронски новац?	6
2. Е-БАНКАРСТВО	9
3. КАРТИЦЕ	12
3.1. Историјски развој картица.....	12
3.2. Паметне картице	15
3.3. Банкомат.....	16
3.4. ПОС терминал.....	17
4. НОВАЦ НА ИНТЕРНЕТУ	18
4.1. Мултифункционални системи плаћања	20
4.2. PayPal систем	21
4.3. Cyber Новац.....	23
5. СИСТЕМИ ВЕЛИКИХ ПЛАЋАЊА	24
5.1. Платни систем САД – Систем Федералних Резерви	25
5.2 Fedwire	25
5.3. Аутоматед Цлеарнинг Хоусе (АЦХ).....	26
5.4. CHIPS(Clning Hoyse Interbank Payments System).....	26
5.5. SWIFT (Society for Worldwide Interbank Financial Telecommunication).....	28
5.5.1. Концепција и организација SWIFT мреже	29
6. МИКРОПЛАЋАЊА.....	30
6.1. Millicent.....	30
6.2. Netbill	32
7. МОБИЛНА ПЛАЋАЊА.....	33
7.1. Мобилни финансијски сервиси	33
7.1.1. Банкарски сервиси.....	33
7.1.2 Брокери.....	33
7.1.3. Инвестиционо Банкарство	34
7.2. Принцип пословања мобилног банкарства	34
7.2.1. Стратегије мобилног банкарства	35
7.2.2. Техничка инфраструктура мобилног банкарства.....	36
7.3. Сигурност.....	36
7.4. Пример мобилне банкинг апликације	37
8. БЕЗБЕДНОСТ ПОСЛОВАЊА НА ИНТЕРНЕТУ	38
ЗАКЉУЧАК	43
ЛИТЕРАТУРА.....	45

УВОД

Интернет, као и остала достигнућа технолошког развоја, изазвао је најизразитије промене у финансијском сектору и створена је могућност да клијенти буду сами своји банкари и да својим средствима располажу у сваком моменту онако како желе! Претходно поверење јавности у новац је било утемељено у самој физичкој опипљивости новца (метал, папир...). Данас, када говоримо о дематеријализованом новцу који није ништа друго до софтверски производ, поверење се мора поставити на сасвим другим основама тј. на технологију која подржава трансфер тих невидљивих (софтверских) средстава. Јавности једино преостаје да верује инфраструктури којом овај новац циркулише. Када се говори о поверењу јавља се као основни проблем сигурности. Људи се плаше да трансферишу новац кроз Интернет јер могу постати мета криминалних активности од стране неауторизованих особа. Због тога сигурност тих модела свремене комуникације мора бити на веома високом нивоу.

Промет остварен електронским пословањем, сваке године је све већи. Сврха преласка на електронски начин пословања је оптимизација пословног процеса, унапређење односа између банке и клијената, као и најзначајније остваривање профита пружањем врхунских услуга клијентима. Самим тим и поштовањем њиховог времена, штедњом њиховог новца кроз смањене провизије путем електронских услуга. Кључни успех електронских канала је да се обезбеди сигурност и поверење клијената. Да би клијенти прихватили електронске трансакције неопходно је да имају поверење и осећај да контролишу употребу својих личних података.. Сигурно ће наставити да се развија и модификује захваљујући напретку технологија и потребама клијената.

Појава пластичних картица и дигиталног новца учинили су преокрет ка тоталној дематеријализацији и виртуализацији новца.

Интернет, е – банкарство и мобилно банкарство су довели до тога да је банка изашла из својих просторија. Кроз историју корисник је увек морао да одлази у просторије банке како би обавио посао. Данас банка долази у кућу корисника или на његово радно место. Мобилно банкарство иде корак даље, и преноси банкарске послове у џеп корисника потпуно независно од локације на којој се он налази.

1. РЕАЛНИ НОВАЦ У CYBER ПРОСТОРУ

Пре било каквог разматрања о историји новца или његовим карактеристикама потребно је знати његову дефиницију, тј. да новац представља нешто што је генерално прихваћено као медијум за размену, мера вредности и средство за плаћање. Кроз историју људског рода новац је био стални пратилац човека од праисторије до данас. Размена је увек представљала важан сегмент делатности а системи који су омогућавали ту размену временом су се мењали и усавршавали како је и сам човек усавршавао своју технологију којом се окружио. Развој новца је текао кроз: бартер, медијум за размену, ситан новац, папирни новац, обележени новац и дематеријализовани новац.

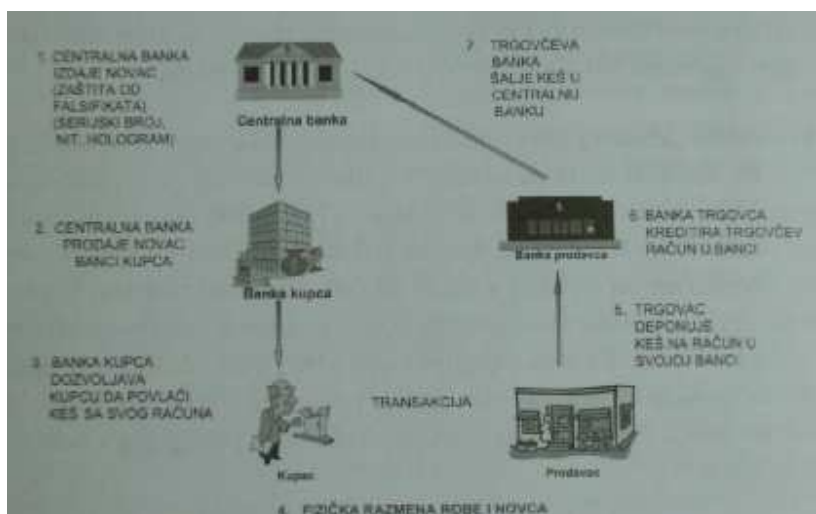
Разумљиво је да успешност једне привреде зависи од тога како се односи према новчаној маси. На сопственом примеру могли смо да научимо које су последице хиперинфлације 1993. године. Огромна маса новца која се сваког дана размени и трансферује, ствара велике тешкоће у манипулацији њиме уколико је у кешу. Неопходност која се намеће је да се новац дематеријализује како би трошкови његовог сервисисања били сведени на разумну меру.

Основна идеја и проблем пословања у субер простору је како обезбедити да се новац пребацује преко електронских комуникационих канала и преко Интернета. Сама идеја представља проблем јер се новац у класичном смислу не може трансферовати преко мреже. То је први разлог што је настала потреба за масовном употребом дигиталног новца као једино средство које је могуће трансферовати кроз рачунарску мрежу. Први проблем који се одмах јавио био је да банке нису спремне за обављање тренутних трансакција преко електронских канала и Интернета. Други проблем био је сигурност на мрежи. Интернет који је прављен за рад у академском окружењу није предвиђен за транспорт финансијских података. Трећи проблем се састојао у томе да није постојала добра комуникација између кредитних/дебитних картица, банковних рачуна и система плаћања. Овакво стање морало се у ходу превазилазити јер је пословање на мрежи диктирало тренутне захтеве. Веома рано су се јавили први приручни системи плаћања који су представљали принудно решење, али у недостатку бољих и они су прихватани. Тек када је схваћен потенцијал Интернет пословања, кренуло се у озбиљан развој система плаћања. Временом и стицањем искуства искристалисали су се захтеви које мора да испуни сваки систем плаћања на Интернету. Дакле, цивилизација је из једне крајности стигла у другу крајност. Крајњи експонент информације о вредности робе је дигитални новац или електронски новац који се може дефинисати као информација о монетарној вредности коју је могуће трансферисати кроз рачунарске мреже, тј. ван уобичајних канала плаћања које традиционално подржавају банке.

Дигитални новац је кулминација процеса дематеријализације новца и његово претварање у информацију која једино постоји „он лине“. Пре појаве Интернета електронски новац је представљао ствар банке, њене техничко – технолошке инфраструктуре и корисник скоро да није био свестан његовог постојања. С појавом Интернета и његовом масовном применом у доменима плаћања и банкарских функција, електронски новац је постао део свакодневнице и тек онда су се поставила питања која су од животне важности а везане су за њега. Иако постоји више модела електронског новца који теоријски задовољавају или се у пракси примењени, још увек постоји читав

низ проблема које он мора да разреши да би за кориснике био прихватљив и како би заменио постојећи „класични новац“.

Да би заменио „класични новац“ електронски новац мора бити универзално прихватљив, што значи да може да се даје из „руке у руку“, и да функционише на веб платформи. Трансакције рађене електронским новцем морају бити јефтиније од класичних трансакција, издавања новца, његово сервисирање и коришћење морају бити јефтиније од рада класичним новцем. Уопштено говорећи, дигитални новац мора пружати знатне предности како би од корисника био широко прихваћен. За сада, дигитални новац само у одређеним сегментима успешно замењује класичан, али тамо где је прихваћен обезбеђује велику брзину протока новца. Разлог за мању неприхватљивост електронског новца је у томе што у многим случајевима, да би се понудио и прихватио електронски кеш, мора да се изврше провере стања на рачуну или кредитне способности онога ко нуди електронски новац. Код класичног новца онај који нуди новац не мора да доказује ништа и никоме јер новац који нуди сам је за себе доказ. Свако може да понуди или да га прихвати без икакве провере а трансфер је једноставан. Ово је несумњива предност класичног новца која још дуго неће (или никад) бити превазиђена.



Слика 1. Трансакција са готовим новцем

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

Чињеница је да дигитални новац све више добија на значају. Интернет као огромни пословни потенцијал захтева дигитални новац и уопште није спорно да ће се његова употреба све више ширити. Да би задовољио кориснике мора да испуни неке услове. Мора бити лако преносив, да трошкови његовог креирања и руковања буду мали или

¹ Слика 1. Трансакција са готовим новцем

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

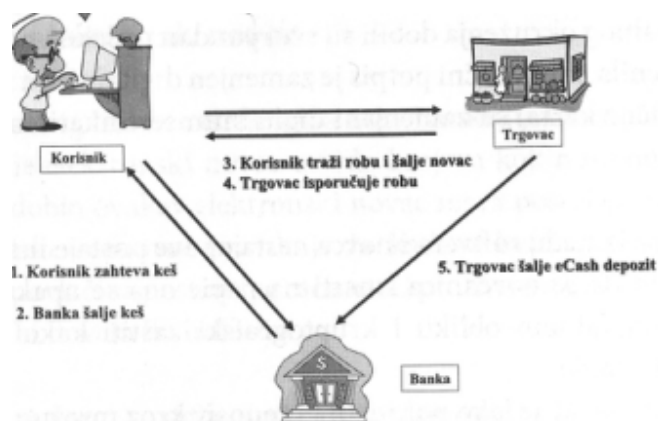
бар мањи од класичног новца, мора да омогућава промет без посредника, тј. да се са њиме може радити „офф лине“ трансакције. Посебно мора да се обезбеди анонимност учесника у трансакцији.

1.1. Како настаје електронски новац?

Систем електронског новца настаје када нека банка емитује новац у виду бројева који носе одређену вредност. Да би се добио овакав електронски новац мора постојати рачун код ове банке и основно правило је да када се купује електронски новац, прави новац се ставља на резервацију или се повлачи са рачуна. У противном би се повећавала новчана маса $M1/2$, неравно и неосновано, што би доводило до инфлације. Електронским новцем се даље може плаћати трговцу за производ или услуге, а трговац га може депоновати у било којој банци која учествује у конкретном систему електронског новца или га може проследити другом трговцу. Трговац у сваком тренутку може да провери исправност електронског новца контактирајући банку која га је емитовала. Корисници који су заинтересовани за плаћања електронским новцем у већини случајева морају да инсталирају посебан софтвер на свом рачунару који им омогућава да комуницирају са банком као и да подижу новац са свог рачуна у банци а затим га пребаце у свој Електронски новчаник на рачунару. Приликом плаћања, они размењују е-новац са трговцем у замену за производе или услуге које желе да купе. Банка која прима депозите у електронском новцу откупљује новац који је трговац добио. Друга варијанта је да корисници имају Паметну картицу и да приступају банци преко Интернета тако да се вредност новца пребаци на картицу а затим се та вредност или новац користи за плаћање.

У реалном окружењу корисник одлази у банку и са свог рачуна подиже одређену суму новца. Благајник или банкомат га исплаћују, одлази у трговину и плаћа робу. Трговац после предаје пазар банци и тако је затворен круг. Овакав протокол плаћања је у потпуности истоветан плаћању дигиталним новцем. Протокол плаћања електронским новцем има три фазе:

- Повлачење новца (withdrawal)
- Плаћање (payment)
- Депозит (deposit)



2

Слика 2. Основни протокол плаћања

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

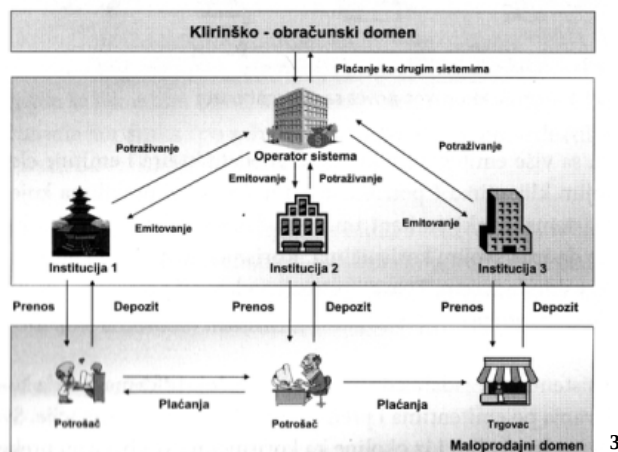
С обзиром на то да су модели електронског новца још увек новост, постоји доста различитих приступа, како техничких тако и технолошких и организационих. Модели електронског новца се разликују по: технологији, учесницима, емитентима, трговцима.

Постоје и две основне технологије уписа новчане вредности: вредност се налази на смарт картици или се налази у софтверском новчанику на рачунару. Трећа варијанта може да се јави као комбинација прве две. Учесници у систему плаћања и организација пословања може бити различита али су учесници следећи: Емитенти електронског новца, Оператори/процесори, Корисници, Трговци, Куће за клиринг трансакција електронским новцем. Најзначајнији су емитенти електронског новца. Мрежни оператори и добављачи обезбеђују техничку подршку док су институције за клиринг обично банке или специјализоване институције у власништву банака. Може бити један или више емитената у зависности како је систем организован.

У систему са једним емитентом, токови вредности су слични онима који се обављају у реалном систему који се састоји од једне емисијоне институције (централне банке), банкарског система и малопродајног система. Емитент је тај који креира електронски новац и емитује га учесницима и финансијским институцијама. Финансијске институције даље преносе електронску вредност корисницима а они их даље користе за плаћање. Новац циркулише међу учесницима и користи се за плаћања трговцима. Трговци са своје стране када добију новац депонују га у своју банку која такође мора да буде члан система електронског новца. Новац бива пребачен са рачуна корисника на рачун трговца и тиме је електронска новчаница или вредност завршила пут.

² Слика 2. Основни протокол плаћања

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

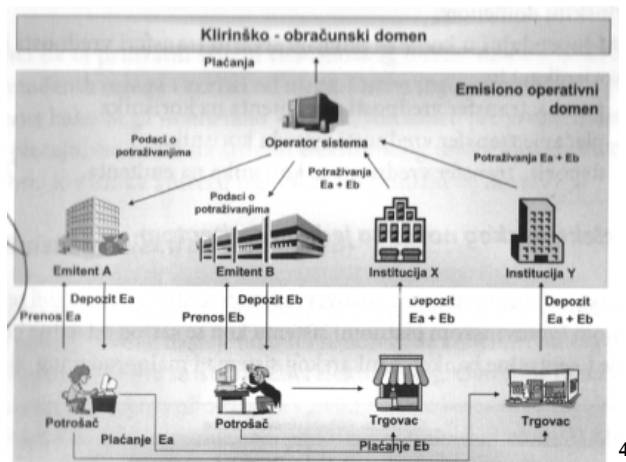


Слика 3. Систем електронског новца са једним емитентом

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

Систем са више емитената функционише мало другачије. Заправо сваки од емитената креира и емитује електронски новац својим клијентима у складу са правилима које дефинише оператор система. Сваки емитент има одређену количину електронског новца коју може да изда својим корисницима. Корисници међусобно обављају плаћања електронским новцем. Трговци примају уплате од потрошача и депонују ова средства код институција – учесница.

Оператор система има задатак да прима и прослеђује информације, да консолидује потраживања по емитентима и преноси им релевантне информације. Сва плаћања из система ка околини и из околине ка корисницима се обављају преко клириншко – обрачунског домена.



³ Слика 3. Систем електронског новца са једним емитентом

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

⁴ Слика 4. Систем електронског новца са више емитената

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

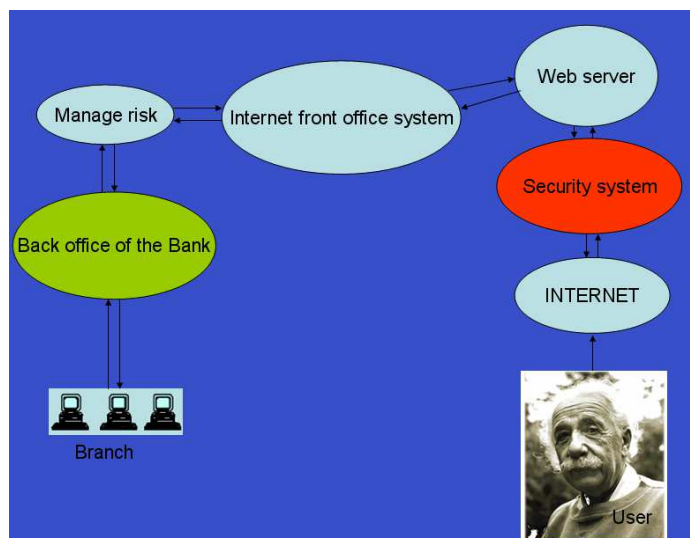
Слика 4. Систем електронског новца са више емитената

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

2. Е-БАНКАРСТВО

Како би финансијска трансакција могла да се обави преко Интернета потребно је да у технолошком ланцу плаћања буде укључена нека банка или финансијска организација преко које ће се извршити пренос новца. Ово надаље значи да су банке од самог зачетка биле укључене у читав посао Е-commerce. У почетку се оне јављају као носилац картичарства а затим стављањем неких својих сервиса на располагање корисницима банке постају активни учесници у пословању преко Интернета. Може се рећи да су банке централно место где се финансијски затвара пословање, пребацивањем средстава са рачуна купца на рачун продавца.

Технолошко банкарско пословање са корисницима започето је аутоматизацијом на нивоу шалтерског пословања. Прво су у шалтер сали инсталирани рачунари како би се убрзали послови рада са грађанима. Затим су постављени банкомати са циљем да се превазиђе ограничење радног времена експозитура и корисницима стави на располагање сет услуга 24 часа дневно. Следећи ниво је аутоматизација трговинских трансакција увођењем картица и увођењем ПОС терминала. Развојем технологије великим корисницима – фирмама је омогућено да приступе директно банци и обављају послове преко изнајмљене линије и преко конекције директно са банкарским апликацијама. За стављање сервиса на располагање корисницима преко Интернета било је потребно да се развије технологија која ће повезати канцеларију банке и кориснике који банци прилазе преко Интернета. Створен је средња канцеларија и његов задатак је да прихвати кориснике са Интернета и да сервисира њихове захтеве. Средња канцеларија комуницира са банкарским апликацијама преко заштитног зида система. Спољашњи корисници могу приступити банци преко различитих комуникационих канала, почев од Интернет приступа, мобилних уређаја или преко интерактивне телевизије. Сви ови канали омогућавају приступ Средњој канцеларији система и даље улазе у систем банке где им се ставља на располагање сет послова у зависности од привилегије коју су добили од банке.



Слика 5. Модел банке на Интернету [1]-Eng/Srb(Branch-Огранак, Back office of the Bank-Канцеларија банке, Manage risk- Управљање ризиком, Internet front office system- Интернет систем, Web server- Интернет сервер, Security System- Систем Обезбеђивања, Internet- Интернет, User- Корисник).

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

С обзиром на то да је за развој овог посла било потребно разградити техничко – технолошку инфраструктуру, банке су ту исту мрежу почеле да користе за стављање на располагање неких чисто банкарских сервиса, као што је упит стања на рачуну и слични сервиси. Даљим технолошким развојем и увођењем смарт картица стекли су се сигурни услови да се већи број сервиса ставе на располагање, па и да се обаве одређена плаћања путем Интернета. Логика код модела банке на Интернету је да се сви послови одвијају паралелно уз потпуну синхронизацију свих послова из реалног окружења и са Интернета. Корисник у експозитури обави трансакцију и одмах након тога може преко Интернета да провери промену. Када приступа преко Интернета корисник прво наилази на систем идентификације где се најчешће за идентификацију и ауторизацију најчешће користи смарт картица или у неким другим случајевима користи мини ЦД. И у једном и у другом случају корисник мора да има лозинку како би се спречило да се неко други уместо њега пријави и обради трансакцију. Када прође систем заштите корисник долази на веб сервер где му на располагању стоји одређени сет услуга које може самостално да обави. Избором захтеване трансакције улази у процедуру и попуњава одређену форму или део апликације који је потребан да се трансакција уради, након тога затвара апликацију тј. одјављује се. Основни разлог за коришћење е-банкарство сервиса, за корисника је уштеда времена, смањење напора и трошкови одласка у банку. Велики број послова финансијске природе захтева често присуство у банци, путовање до ње а затим чекање у реду, време обављања трансакције или добијање обавештења, а све то тражи доста напора, времена и новца. Стављањем одређених банкарских сервиса на Интернет растеређено је шалтерско пословање (сектор становништва), редукују се

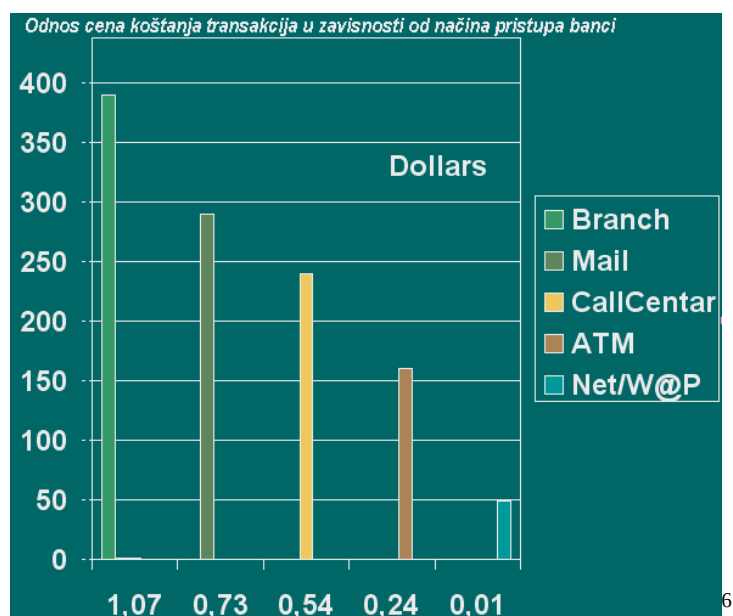
⁵ Слика 5. Модел банке на Интернету [1]

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

доласци корисника у банку, а уједно се стварају услови за повећање обима пословања без потребе додатног интересовања.

У овом случају показало се да је Интернет стратегијска предност банака како би повећале своју оперативност, побољшале квалитет услуга, и уједно редуковале трошкове пословања. Поред већ наведеног постоји низ других разлога за ову врсту аранжмана : стварање имица иновативне фирме, боље и веће интерактивне могућности, могућност рационализације потенцијала банке, промоција самоуслужног банкарства, доказ о банкарским конкурентским могућностима . . .

Сви претходни разлози за увођење Интернета у банкарско пословање су споредни у односу на цену коштања по трансакцији. Са дијаграма се види да цена трансакције која је одрађена преко Интернета и мобилних комуникација за 97% јефтинија од трансакција у експозитури. Корисник је сам свој ликвидатор – благајник, користи свој рачунар који одржава, сноси одговорност и све трошкове у конекцији са рачунаром банке.



Слика 6. Однос цена коштања трансакција у зависности од начина приступа банци [6]

Eng/Srb (Branch- Грана, Mail- Пошта, CallCentar-Позивни Центар, ATM- Банкомат, NET/W@p- Интернет).

Интернет: <http://www.etrgovina.org>

Основни задатак банке као институције ја да прикупља слободна средства од грађана и да их даље пласира. Да би то постигла и привукла што више штедиша она мора да ствара повољну слику о себи јер на тај начин увећава приходе и број комитената. То

⁶ Слика 6. Однос цена коштања трансакција у зависности од начина приступа банци [6]

Интернет: <http://www.etrgovina.org>

значи да банка мора да успостави и негује добре односе са својим клијентима. Примена Интернета довела је до стварања веће конкуренције, промена односа снага корисника и банака, развој међубанкарске конкуренције која даје моћ клијентима, потпуно отклањање географски препрека у финансијском пословању.

Основне карактеристике е-банкарство сервиса су:

- Индивидуалност
- Мобилност
- Независност времена и места
- Флексибилност
- Интерактиван рад

Наведене карактеристике стварају веома повољне услове за развој виртуалног банкарства и ширења његове примене у другим областима, али основни услов који мора бити испуњен да би е банкинг могао нормално да функционише је поуздана, брза и разграната техничко – технолошка инфраструктура. Електронски новац може бити искоришћен ефикасно и делотворно једино ако постоји инфраструктура која је опремљена техником која је на високом нивоу. Велика брзина преноса података је предуслов за слање информација потенцијалним корисницима. Мора бити омогућен брз, једноставан и економичан приступ свим подацима и сервисима који су стављени на располагање корисницима. Крајњи корисници морају минимално имати ПЦ рачунар са одговарајућим софтвером и системом заштите. Дигитални систем плаћања може бити ефикасан само ако је укључен већи број заинтересованих и ангажованих људи. Сви они у ланцу имају свој део учешћа у послу.

3. КАРТИЦЕ

Кредитне/дебитне картице као медијуми плаћања у традиционалном систему плаћања на мало, у развијеним земљама постоје и функционишу дуги низ година. У нашој земљи њихова употреба била је прилично скромна, тако да јавност није упозната са основним појмовима и процесом плаћања путем кредитних/дебитних картица. Мада се кредитне/дебитне картице данас у свету увелико користе за електронску трговину преко Интернета.

3.1. Историјски развој картица

Кредитна картица се обично дефинише као мали комад пластике који садржи неко средство за идентификацију, што омогућава особи на коју картица гласи да купује робу или услуге на терет свог рачуна, који се периодично задужује. Кредитне картице појавиле су се у Сједињеним Државама током двадесетих година прослог века, када су поједине фирме, попут нафтних компанија и ланаца хотела, почеле да их издају својим потрошачима. Овакве кредитне картице биле су затвореног типа, тј. могле су да се користе само у продајним/услужним објектима компаније која их је издала. Њихова употреба значајно је повећана након II светског рата.

Прву универзалну кредитну картицу, која је могла да се користи у разноврсним продајним/услужним објектима, издао је Динер' Цлуб, Inc., 1950. године. У овом систему, компанија која послује кредитним картицама (Динер's Цлуб) наплаћује

власницима картица годишњу провизију, а њихове рачуне задужује месечно или годишње. Фирме–кооперанти широм света плаћају провизију за услуге Динерс' Цлуба у распону од 4% до 7% од укупног износа рачуна. Другу значајнију картицу овога типа лансирала је Америцан Ехпресс Компанија 1958. године.

Касније су се појавили банкарски системи кредитних картица, у којима банка одобрава рачун трговца одмах по пријему рачуна о продатој роби, прикупљајући износе који ће бити зарачунати власнику картице на крају уговореног периода. Власник картице овај износ плаћа банци у тоталу или у месечним ратама са обрачуном каматом. Први банкарски систем од националног значаја био је Банк Америцард, који је покренула Банк оф Америца из Калифорније 1959. године. Овај систем лиценциран је у другим државама почетком 1966. године, а од 1976–77 године носи назив ВИСА.

Остале значајне банкарске картице су Мастер Цард (раније Мастер Цхарге) и Барцлау'с. Многе банке које су организовале системе кредитних картица на локалној или регионалној основи одлучиле су да приступе великим националним системима пошто се обим услуга ширио. Ови системи су се касније проширили на све делове света. У банкарским системима кредитних картица, власник картице може да изабере плаћање у ратама, у том случају банка наплаћује камату на неизмирени дуг.

За разлику од кредитне картице, дебитна картица је картица која омогућава свом власнику да купује директним задуживањем свог рачуна.

Кредитне и дебитне картице све више добијају на значају као метод обрачуна за плаћања на мало при куповини одређених роба и услуга. Највеће компаније које послују кредитним картицама организовале су засебне електронске клириншке и обрачунске системе. МастерЦард и Виса имају своје сопствене мреже које се користе за верификацију трансакција широм света. Електронски терминали на месту продаје (системи за електронски трансфер новца на месту продаје/услуге — ЕФТ/ПОС терминали) омогућавају да се подаци са картице провере за мање од 15 секунди у оквиру мреже која повезује трговце широм света са центром за обраду кредитних картица и емитентом кредитних картица.

На пример, систем који користи Виса, ВисаНет, састоји се од три рачунарска центра, од којих су два у Сједињеним Државама, а један у Великој Британији. Широке комуникационе мреже повезују трговце, који користе Виса систем, са овим рачунарским центрима. Ове мреже се све брже шире, упоредо са трендом прихватања кредитних картица од стране потрошача.

Кредитне картице, углавном, захтевају четири стране у свакој трансакцији: власника картице, трговца који продаје робу или услуге, онога ко врши обраду плаћања кредитном картицом и емитента кредитне картице.



Слика7. Картице[7]

Интернет: <http://www.vps.ns.ac.rs>

Платни системи с кредитним/дебитним картицама показали су се крајње неотпорним на злоупотребу. Кредитне/дебитне картице могу се украсти од њихових власника и онда злоупотребити, а трговци који примају плаћања кредитним/дебитним картицама могу преварити потрошача и не испоручити му робу. Губици због злоупотребе плаћања кредитним/дебитним картицама од стране трговаца су значајни. Због тога се врши оштра селекција трговаца који ће добити овлашћење да примају плаћања путем кредитних/дебитних картица. Слично томе, издавање кредитних/дебитних картица све се више контролише како би се смањила злоупотреба и превара од стране власника картица.

Упркос овим проблемима, компаније које послују кредитним/дебитним картицама, као што су Виса и МастерЦард, тренутно су најактивније у развоју безбедних платних система за плаћање кредитним/дебитним картицама преко Интернета. Безбедне методе за трансфер података и обезбеђење ефикасног система ауторизације представљаће велико унапређење у односу на оффлине системе, који се тренутно користе за продају робе широке потрошње и услуга преко телефона или факса. Међутим, кредитне и дебитне картице створене су у време када је нагласак у индустрији финансијских услуга био на аутоматизацији трансакција. Кредитне/дебитне картице представљају превише гломазан и ограничени систем, тако да је мало вероватно да ће се на њима заснивати један заиста глобални и електронски платни систем будућности за плаћања на мало, упркос почетном успеху који трансакције кредитним/дебитним картицама преко Интернета тренутно бележе.

Процес плаћања- рекли смо да трговци имају однос са неком пословном банком или независном продајном организацијом, преко којих врше обраду трансакција кредитним/дебитним картицама.

Трговци морају да плате пословној банци или независној продајној организацији дисконтну провизију засновану на укупном износу продаје. Слично томе, пословна банка или независна продајна организација мора да плати емитенту картице провизију за замену онда када изврше обраду рачуна трговца. Наравно, ово је само груба скица једног много комплекснијег процеса, који се у стварности одвија.

⁷ Слика7. Картице[7]

Интернет: <http://www.vps.ns.ac.rs>

Уобичајена трансакција помоћу кредитне картице одвија се на следећи начин:

Трговац израчунава вредност купљене робе и тражи од купца да плати. Купац даје трговцу картицу. Трговац провлачи кредитну/дебитну картицу кроз ПОС терминал. Вредност продате робе се уноси ручно, или се преузима из регистар–касе. Трговац подноси податке о картици и вредности купљене робе својој пословној банци, са захтевом за ауторизацију. ПОС терминали су обично подешени тако да захтевају ауторизацију у моменту продаје, а стварни пренос података са рачуна врши се касније. Пословна банка затим обрађује трансакцију, прослеђујући захтев за ауторизацију банци која емитује кредитну/дебитну картицу. Број картице идентификује врсту картице, банку која ју је емитовала и рачун власника картице. Ако власник картице има довољно новца на свом рачуну да покрије куповину, банка која емитује картицу ауторизује трансакцију и генерише ауторизациону шифру. Ова шифра се шаље назад пословној банци. Банка која емитује картицу резервише новац на рачуну власника картице у износу који је еквивалентан вредности купљене робе. Међутим, рачун власника картице се још увек не задужује.

Пословна банка обрађује трансакцију, а затим шаље шифру за одобрење или одбијање ПОС терминалу трговца. Сваки ПОС терминал има свој јединствени идентификациони број, тако да је институција која врши обраду трансакција у могућности да проследи податке управо том терминалу. Рачун штампа ПОС терминал или регистар–каса. Трговац захтева од купца да потпише рачун, који га обавезује да надокнади назначени износ банци која емитује кредитну/дебитну картицу.

Касније, када се радња затвара, трговац упоређује ауторизације које су меморисане у ПОС терминалу са потписаним рачунима. Када изврши проверу подударности свих ауторизација са потписаним рачунима, трговац ће превести, или пренети податке о свакој ауторизованој трансакцији кредитном/дебитном картицом пословној банци на депозит. Исто тако, он може депоновати код банке и реалне, потписане папирне рачуне.

Пословна банка, за сваки поједини рачун, врши са одговарајућом банком која је емитовала картицу оно што се назива заменом. Банка која је емитовала картицу одобрава пословној банци износ конкретног рачуна, умањен за износ провизије за замену.

Пословна банка затим депонује износ свих рачуна које је поднео конкретни трговац на његов рачун, умањујући га за дисконтну провизију.

Овај преглед, наравно, није комплетан јер не покрива улогу финансијских мрежа. Он се односи углавном на трансакције Виса и МастерЦард картицама. Код Америцан Ехпрес и Дисцовер картица, на пример, не постоји емисиона банка. Ипак, поменути редослед активности нам може послужити као прилично веран пример једног процеса плаћања картицом.

3.2. Смарт картице

Смарт Цард је пластична картица величине обичне кредитне картице какве су нам присутне у свакодневном животу, с тим да у себи има уграђен чип на којем се налазе процесор, меморија (РАМ и РОМ) и елементи који омогућавају комуникацију односно размену података с околином. Чип је управо оно што ове картице чини смарт. Ова веза

између прикладне пластичне картице и микропроцесора омогућава нам да се велика количина података може пребацивати, обрадити било онлине или оффлине.

Смарт картице могу пренети неколико стотина пута више података него досадашње обичне картице с магнетском траком. Информација или апликација пребачена на чипу у картици преноси се помоћу уграђеног склопова до терминала или читача картице.

У зависности од тога какав је чип уграђен у картицу разликујемо два типа картица: меморијске картице и процесорске картице. Меморијске картице су оне код којих је у чип уграђена само меморија. Такве меморијске картице могу пренети велику количину података од обичних картица с магнетском траком. Због сигурносних разлога примена оваквих картица ограничена је на оне апликације код којих сигурност података не игра велику улогу. Овакве картице обично се користе у једноставним апликацијама као што су телефонске чип картице. Процесорске картице су картице које осим меморије на чипу имају уграђен микропроцесор, па према томе могу обављати различите функције као што су енкрипција података, напредна сигурност података, локална обрада података, комплексне операције над подацима итд. Због додане процесорске интелигенције, величине и могућности обраде података, може пружити већу сигурност и има велику примену у различитим подручјима.

Сигурност је једно од најважнијих обележја Смарт картица. То је често од примарне важности, посебно код финансијских апликација, и када је у питању приватност података. Смарт картица са својом уграђеном интелигенцијом, способна је да претрпи разне нападе од стране неауторизираних особа које имају намеру преваре или читања поверљивих података смештених на картици. Предности су у сигурности, интегрисаности, свестраности и економичне погодности.

Смарт картице постају све више значајније и одиграће важну улогу у нашем свакодневном животу. Ускоро можемо очекивати универзалне Смарт картице које ће се користити као личне карте, здравствена картица, кредитна картица, возачка дозвола, картица за коришћење мобилних и банкомат уређаја, картица за приступ сигурним мрежним сервисима, улазница за библиотеку или биоскоп и још много тога.

3.3. Банкомат

Један од важнијих облика електронских канала је банкомат (енгл. Automated Teller Machine – АТМ). У зависности од модела банкомата, овај уређај може клијентима пружати услуге подизања готовине, уплаћивања депозита, пребацивања средстава са једног рачуна на други, и провере стања на рачуну. Велика предност оваквих уређаја представља њихова 24-часовна доступност.

Корисник долази до банкомата, бира са менија на екрану посао који жели да обави и ставља картицу у слот банкомата. Банкомат чита картицу и после провере исправности нуди кориснику сет услуга за које је предвиђен. Корисник се аутентификује помоћу ПИН-а који се добија уз картицу, а затим уноси износ који жели да подигне. Банкомат проверава да ли се трансакција може извршити, ако су средства расположива банкомат ће дозволити трансакцију на тај начин што враћа картицу, броји новац и штампа слип. У противном емитује поруку да је трансакција неуспешна и враћа картицу. У случају грешке (нпр. грешка ПИН-а 3 пута) банкомат ће задржати картицу у слоту банкомата, како би се и даље неометано рад одвијао, а картица се може подићи поново у

експозитури. Исто тако корисник мора да узме новац у одређеном временском периоду јер ће и он бити поново враћен у банкомат ако је корисник заборавио да га узме.



Слика 8. и 9. Слот за картицу у банкомату и ПОС (Point of sale – Продајни пункт) уређај [6]

Интернет: <http://www.vps.ns.ac.rs>

3.4. ПОС терминал

ПОС терминал се поставља на продајним местима и служи за аутоматизацију процеса плаћања.

ПОС терминал се конектује на телефонску линију тако да телефонски апарат може нормално да се користи током радног времена. Само у тренутку покретања трансакције ПОС заузима телефонску линију и одмах по завршетку прекида везу и ослобађа линију. ПОС терминали се углавном добијају од банке на коришћење приликом склапања уговора између трговца и банке. Банка задржава право да ако је недовољно искоришћен ПОС повуче или наплати неки минимални износ као накнаду за његове трошкове одржавања. Када трговац добије ПОС терминал банка је дужна да га постави, повеже са процесинг центром и да обучи особље трговачког места. Радни дан почиње тако што трговац повезује ПОС са процесинг центром и скида све потребне податке. Клијенту се пружа услуга да код трговца може плаћати робу картицом. Трговац провлачи картицу кроз ПОС терминал и штампа рачун у два примерка. Један примерак потписује клијент, а други се качи за фискални рачун. У случају злоупотребе ПОС ће одбити трансакцију. На крају дана се ради филе трансфер. То је рекапитулација свих дневних трансакција када се ради измена свих података са процесинг центром. У том тренутку се усаглашавају сва стање а ПОС штампа “дневно стање” са свим трансакцијама.

⁸ Слика 8. и 9. Слот за картицу у банкомату [6]

Интернет: <http://www.vps.ns.ac.rs>

⁹ ПОС (Point of sale – Продајни пункт) уређај

Интернет: <http://www.vps.ns.ac.rs>

4. НОВАЦ НА ИНТЕРНЕТУ

Увођењем Интернета у пословне процесе дошло је до драстичне промене у начину пословања. Пре свега, информациони системи банака нису били припремљени за овакав начин рада, па су се у банкарском пословању појавиле фирме које су нудиле послове аутсорсинга (АСП – Application Service Provider). Ове фирме су преузимале одређене послове и радиле их за потребе банке али су ти послови рађени ван банке. Ово је довело до повећања ризика пословања банке.

Примене рачунара у банкарском пословању 70-их година прошлог века довело је до великих промена. Карактеристика ових система била је да су терминали били директно везани за централне јединице и сваки прекид комуникације представљао је застој у раду. Ипак и овако конципирани системи су омогућили стварање јединственог информационог система у банкама. Појавили су се први он лине системи. Следећи виши ниво повезивања банака остварен је преко клијент – сервер архитектуре која је, у односу на претходни систем, била напреднија и омогућавала да у времену када комуникациони канали не раде удаљене експозитуре раде у офф лине режиму тако да, када се комуникација успостави клијент и сервер размене податке и усагласе их и наставе синхронизовано да раде.

Када се говори о технологији, системима и механизмима рада треба напоменути да су системи електронског плаћања тренутно у експанзији. Ако се зна да је више од 6000 различитих система у употреби, онда је тешко груписати их по технолошким решењима. Ипак, генерално су груписани на системе базиране на рачунима, системе са платних картицама и системе замене готовине.

Када се говори о моделима плаћања ту се пре свега мисли на то ко покреће трансакцију и како се она одвија до свог завршетка.

Метод плаћања кешом - Трансакција се започиње тако што на основу захтева корисника банка издаје новчаницу коју корисник прослеђује до трговца а овај доставља банци, где се она затим поништава. Новац може да буде на рачуну банке или на рачуну корисника и да у оба случаја банка је та која даје одобрење за коришћење новца. Овај метод у потпуности имитира циклус реалног новца.

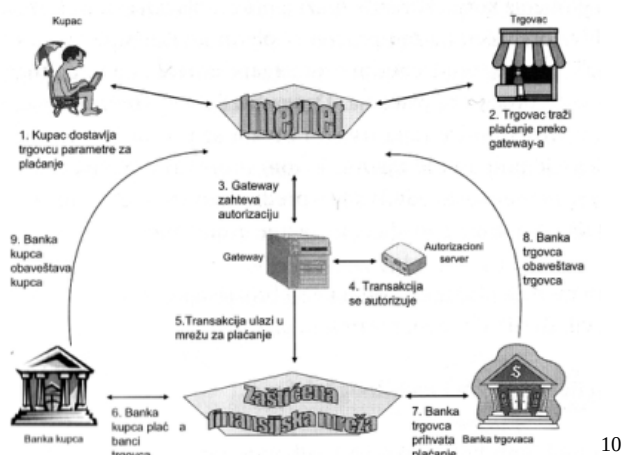
Метод чека. У овом моделу пословања трансакцију започиње корисник који на свом рачунару формира чек и даље га прослеђује на наплату. Чек корисник потписује, додаје сертификат картице и банке и пакује га у дигиталну коверту. Прималац чека са своје стране прима чек на рачунар, додаје своје податке како би банка знала коме треба да пребаци новац, поново га пакује и шаље банци на наплату.

Модел плаћања са платним картицама. У овом моделу трансакцију започиње корисник тако што приступа сајту трговца и тражи одобрење за плаћање. Трговац га пребацује ка банци где се извршава трансакција а банка само информисе корисника да му је новац скинут са рачуна.

Модел плаћања налогом. Ово је систем који је најчешће примењен у е – банкинг системима. Корисник има инсталиран софтвер на свом рачунару и смарт картицу која има сертификате и дигитални потпис. У комбинацији са ПИН бројем корисник покреће трансакцију дајући налог банци да се са његовог рачуна изврши плаћање.

Куповина, плаћање у банци преко рачуна. Корисник на сајту трговца пронађе жељену робу и број рачуна на који изврши уплату новца. Један примерак уплатнице доставља трговцу или га е-маилом обавести да је уплатио новац, овај провери уплату, а затим му робу доставља на назначену адресу. Овај начин плаћања је неповољан за купца јер мора да иде у банку.

Плаћање путем картице. Ово је најпогоднији метод али уз одређену дозу ризика, како за купца тако и за трговца. За овакав начин пословања потребно је обезбедити квалитетне сигурносне методе плаћања. Добра страна овог начина плаћања је што корисник у тренутку када пронађе оно што је тражио може одмах да плати, а за кратко време на назначену адресу добије поручену и плаћену робу. Са становишта трговца ово је добар метод јер истог тренутка када је роба поручена, добијен је и новац за њу. Купац је ово најкомфорније плаћање. Овај начин плаћања захтева значајно повећање броја учесника у процесу плаћања. Процедура рада је следећа: корисник преко Интернета проналази трговца и на његовом сајту бира робу. Са своје стране трговац омогућава кориснику да он претражује његов сајт, чекира робу и формира „потрошачку корпу“. Када је корисник завршио са пуњењем корпе, дакле направио је тотал за плаћање, прелази у следећу фазу, а то је плаћање. Кориснику се на сајту нуди избор којом ће картицом обавити плаћање.



Слика 10. Модел плаћања са картицама [1]

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

Корисник бира картицу. У том тренутку корисник напушта сајт трговца и прелази на сајт „процесора плаћања“ и активира ССЛ. Процедура се даље наставља тако што се кориснику отвара страница за пријаву на систем за плаћање. Ок корисника се тражи да попуни следеће податке: име, презиме, јмбг, бр картице, датум важности и ПИН број. Када је све испуњено даљу процедуру преузима процесор плаћања. Први ниво провере

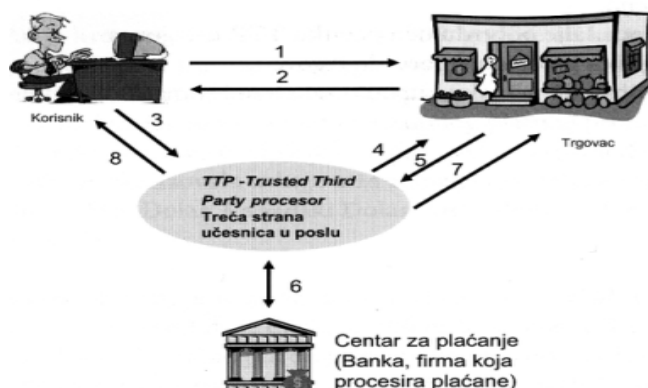
¹⁰ Слика 10. Модел плаћања са картицама [1]

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

је провера података који су унети. Ако су сви подаци исправни проверава се ПИН код и ако је и то исправно процедура се наставља тако што се проверава стање на рачуну у банци кроз посебну заштићену мрежу. Уколико је стање на рачуну позитивно трансакција се одобрава, шаље се процесору плаћања и он даље обавештава стране учеснице у трансакцији да је све извршено регуларно. Процесор генерише број под којим се води трансакција и доставља га кориснику и трговцу. Овај број је значајан зато што ако нешто касније није у реду по њему се обављају рекламације. Овим је сама трансакција плаћања завршена али је остала фаза банкарског пост процесуирања. Пошто је банка кориснику дата средства резервисала, потребно је сад дата средства трансферовати на рачун трговца. Ово се даље ради стандардним поступцима међубанкарских плаћања. Код овог модела плаћања платним картицама постоје две могуће варијанте: тунеловање и прерутирање. Прерутирање подразумева да се корисник са сајта трговца пребацује на сајт процесора плаћања и наставља даље са логовањем и провером, а тунеловање подразумева да се у оквиру сајта трговца отвара прозор који је под SSL –ом и обезбеђује потпуну заштиту. У том прозору се попуњавају подаци и процедура се потпуно исто одвија као у претходном моделу, осим што је у „адресс“ остала иста адреса као да се ништа није променило.

4.1. Мултифункционални системи плаћања

У реалном окружењу корисници често имају потребу да за спровођење одређене процедуре користе трећу страну како би се сигурно спровела одговарајућа трансакција. На Интернету овај метод потврђивања од трећег поверљивог учесника (Трустед Тхирд Парту – ТТП) је уобичајан и он је тај који има задатак само да буде посредник и да утврди аутентичност учесника у пословању. Код овог протокола купац шаље поруку трговцу. Трговац прима поруку и враћа је са захтевом за плаћање. Купац верификује потпис трговца шаљући га у ТТП. ТТП верификује потпис купца и шаље захтев трговцу да потврди наруџбину. Трговац када прими овај захтев верификује ИД број наруџбине и износ који треба да се плати, а затим шаље повратну потврду ТТП-у. ТТП тражи и добија ауторизацију од централе где се држе сви рачуни корисника. ТТП шаље потписану потврду трговцу да је трансакција одобрена. ТТП шаље купцу да је трансакција одобрена и да су средства скинута са рачуна.



11

Слика 11. Плаћање преко трећег поверљивог учесника [4]

Радовановић П., „Перспектива платних система базираних на дигиталном новцу”, Симпозијум: етрговина 2004, Палић

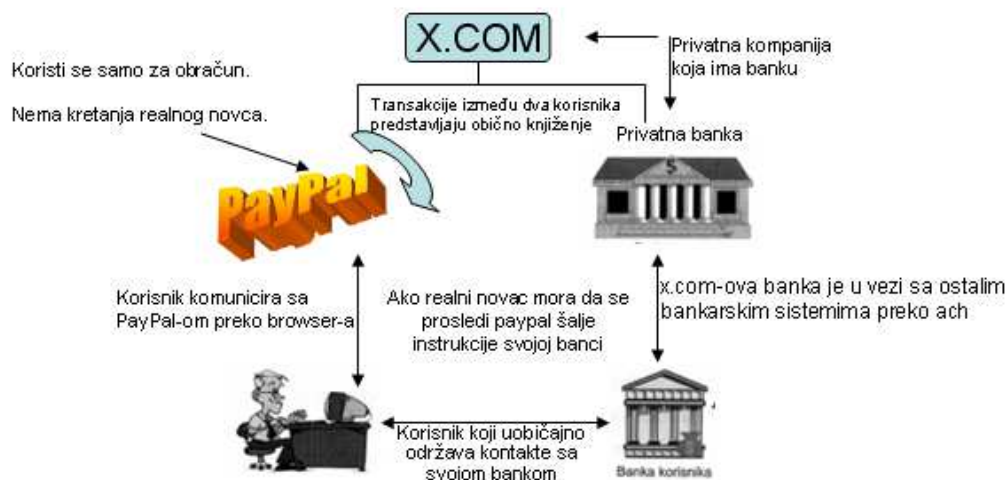
Све стране учеснице у протоколу плаћања имају потврду о обављеној трансакцији. Купац има на свом рачунару захтев трговца за плаћање и има потврду ТТП-а да је оно успешно завршено. Трговац има захтев и ИД број под којим води наруџбеницу и потврду ТТП-а да је трансакција успешно обављена. ТТП има потврду која је потписана од обе стране учеснице у трговини. У систему плаћања ТТП могу бити укључена и два ТТП, један од стране купца и један од продавца. Постоји много мултифункционалних система плаћања, од којих би издвојио **C2C**, **GC Tech**, **CCNOW**, **B2B** а два, по мени, најпознатија ћу и објаснити.

4.2. PayPal систем

PayPal систем је кренуо са радом у марту 1999. године али су тек у октобру исте године започеле прве трансакције. Регистрован је у УСА у држави Делаваре, а 31.12.2001. године имали су 600 запослених. Ту годину завршио је са 12.000 корисничких рачуна и 235.000 долара укупног платног промета. Године 2005. PayPal је процесуирао више од 27 милијарди долара и остварио приход од 1 милијарде. Компанија је локализовала услуге у 14 земаља и подржала плаћање у шест различитих валута USD, CAD, AUD, EUR, JPY, FUNTA. PayPal је систем који ради као посредник на Интернету. То значи да се купци и трговци у тренутку обављања трансакције морају наћи на PayPal -у. Плаћање се може обавити директно са једног PayPal рачуна на други, може се платити кредитним и дебитним картицама или електронским чековима. Плаћање може бити извршено било коме, било где, преко емаила. Посебно је интересантно да је омогућено да се обаве појединачна или групна плаћања. Приликом отварања рачуна код PayPal система, пре свега треба одлучити да ли се отвара лични рачун или се отвара рачун за фирму. PayPal дозвољава својим корисницима да имају један Персонални, Премиер или Бусинесс рачун. У сваком случају, сваки PayPal рачун

¹¹ Слика 11. Плаћање преко трећег поверљивог учесника [4] Радовановић П., „Перспектива платних система базираних на дигиталном новцу”, Симпозијум: етрговина 2004, Палић

мора садржати јединствену е-маил адресу, финансијске или друге релевантне информације. Да би се постао PayPal корисник треба отићи на њихов сајт, ући на страницу за регистрацију корисника рачуна, а затим одабрати опцију, односно ону врсту рачуна која највише одговара. PayPal омогућава све врсте плаћања и пријем новца од појединца или групе људи. Уколико корисник има на располагању више различитих извора средстава PayPal ће исплатити корисников рачун према следећем распореду: Instant Transfer, PayPal купчев кредит, Кредит цард и наком тога е-чек. Све наведено представља погодности које пружа овај систем плаћања, али зарада је основни мотив пословања тако да PayPal има веома добро разрађен систем зараде. Пре свега основни задатак оваквих система је прикупљање и концентрација капитала. Пословна примена овог система захтева пословни рачун и депонована средства на њему. Лична примена овог система, такође подразумева одређена депонована средства код PayPal-а. Овако прикупљена средства омогућавају да се велика сума новца пласира кроз стандардне банкарске канале. После отварања рачуна и полагања новца, даља плаћања су максимално поједностављена али пошто се не користе сва депонована средства у исто време то значи да ће се појавити једна количина слободних средстава која могу да буду даље пласирана кроз банкарске канале. У том случају се емитује један систем плаћања на банкарском тржишту са знатним износом капитала (100.000.000,00 корисника нека је просек салда на рачуну 100 \$ = 10 милијарди \$). Са своје стране PayPal на сва депонована средства плаћа камате. PayPal у свом портфолију услуга нуди интернационална плаћања, издаје своје картице, кредитне и дебитне, прикупљена средства пласирају преко банака. Оно што треба напоменути је да купац приликом куповине не плаћа провизију већ је та обавеза остављена трговцу. Овај систем плаћања је намењен за масовна плаћања преко Интернета и представља један од најчешће примењених метода плаћања. Пословни корисници овог система су дужни да плате фиксни део плус проценат од трансакције. PayPal се састоји од система плаћања и банке која стоји иза њега. Корисник који плаћа другом кориснику може извршити трансакцију на више начина. Заједно поседују рачун у PayPal-у, тада се врши само трансфер са рачуна на рачун. Да плаћа картицом, где ће се због картичарског система обрачунати нека накнада за услугу и е-check где је процедура нешто компликованија јер се плаћање обавља преко Аутоматске клиринг куће (АЦК).



12

Слика 12. Структура PayPal система [3]

Митровић Н., "Е-банк" Сингидунум, Београд, 2005

Предност овог система је што омогућава међународна плаћања, што значи да овај систем има рачуне у банкама других земљама преко којих обавља трансакције. Тачније речено, ако купац из Канаде жели да трансферује новац у Енглеску он може да уради плаћање у канадским доларима док ће систем PayPal извршити плаћање у фунтама. Конверзију ће урадити сам систем.

4.3. Cyber Новац

Cyber Новац је систем који обезбеђује сигурно плаћање. Фирма уствари продаје безбедан пролаз преко Интернета за податке о трансакцијама путем платних картица. Cyber Новац узима податке које шаље трговац, прослеђује их пословној банци трговца на обраду. Cyber Новац ради од априла 1995. године. Cyber Новац систем плаћања заснован је на „ Cyber Новац Новцаник “ програму који корисници морају да инсталирају на свом рачунару и да га користе приликом куповине. Програм обавља енкрипцију и пренос информација о трансакцијама између купца и трговца. Логика система плаћања је следећа. Корисник на свом рачунару има инсталиран софтвер и када покрене процедуру плаћања дигитални новчаник криптује све податке тако да трговац није у могућности да види податке као што су број платне картице. Трговац са своје стране потписује прослеђену поруку, а само је банка у стању да распакује и провери податке о кориснику.

Предност Cyber Новца је што користи јаку енкрипцију за пренос платних информација. У Cyber Новац -у тврде да су они једина компанија која има лиценцу за коришћење 786- битног RSA енкрипционог алгоритма. Повољна је и околност што трговац не може да види број платне картице купца. Уплата стиже на рачун трговца, у

¹² Слика 12. Структура PayPal система [3]

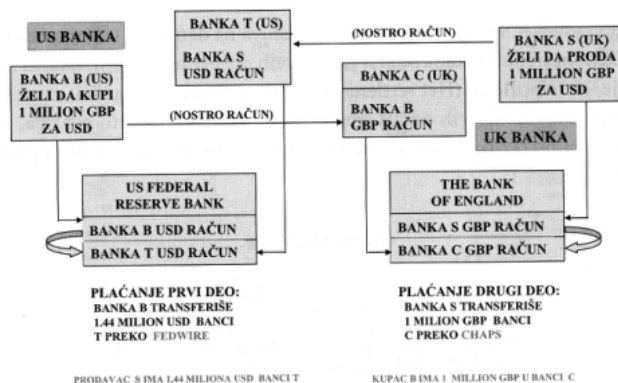
Митровић Н., "Е-банк" Сингидунум, Београд, 2005

року који је уобичајан за трансакције помоћу платних картица. Недостаци овог система се огледају у томе што потенцијални купци/трговци морају имати инсталиран додатни софтвер да би користили систем. То чини овај систем нешто компликованијим за оне који немају довољно искуства у раду са рачунарима. Исто тако трговци морају да имају отворен рачун код неке пословне банке која прима Cyber Новац -ова безбедна плаћања (Сецуре Интернет Паументс).

Треба напоменути да је Cyber Новац једна од првих компанија у области платних система на Интернету.

5. СИСТЕМИ ВЕЛИКИХ ПЛАЋАЊА

Примена рачунара у области банкарства омогућила је појаву електронских трансакција дигиталног типа. Развој електронског банкарства у данашњем смислу речи започео је крајем шездесетих и почетком седамдесетих година двадесетог века. Средином шездесетих година двадесетог века у Великој Британији и САД број трансакција у банкарству се вишеструко повећао тако да примена традиционалних метода обраде трансакција, једноставно, више није била могућа, а проблем је нарастао до те мере да је претио угрожавањем стабилности читавог финансијског система. Владе Велике Британије и САД су, крајем шездесетих година, предузеле мере за аутоматизацију ситних трансакција у банкарству, поготово оних које су репетитивног карактера. На бази идеје, до које су водеће британске банке дошле неколико година раније, у Сједињеним Државама је 1968. године формирана радна група за унапређење размене “без папира” (СЦОПЕ), која је функционисала при Банци федералних резерви у Сан Франциску. Жеља је била да се створи јефтин, поуздан електронски платни систем, као алтернатива чековима. План је био једноставан: претварање периодичних ситних плаћања чековима (као што су зараде или премије осигурања) у посебно обликовану платну евиденцију која ће моћи да се „чита“ уз помоћ рачунара. Резултат ових напора била је прва аутоматска клириншка банка АЦХ –(Automated Clearing House.енг) која је почела са радом 1972. године. Да би једна међународна трансакција могла да се обави обавезно морају да буду укључене две банке и две централне банке, и да једна код друге, међусобно, поседују рачуне. Сва даља плаћања се обављају преко ових рачуна.



Слика 13. Међународна размена [3]

Митровић Н., "Е-банк" Сингидунум, Београд, 2005

5.1. Платни систем САД – Систем Федералних Резерви

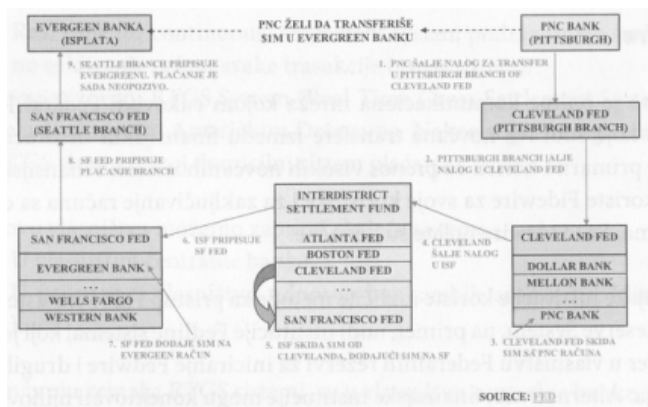
Систем федералних резерви ради као централна банка САД. Систем федералних резерви доноси и спроводи монетарну политику земље у оквиру скупа прописа издатих од владе. Федералне резерве играју централну улогу у контролисању платне инфраструктуре земље (САД) и контролишу различите финансијске институције. Систем се састоји од дванаест регионалних банака Федералних резерви где међу другим функцијама ради национални платни систем. Свака регионална банка ради као депозитна за финансијске институције под чијом је управом. Федералне резерве регулишу ликвидност/компатибилност финансијских институција са постојећим законима и регулативама, такође раде као посредник између банака у закључивању рачуна између платиша и трговца. Један од разлога зашто Федералне резерве играју ту улогу је чињеница да се код њих налазе рачуни финансијских институција. Систем ФР омогућује два примарна начина процесирања електронског трансфера капитала: **Fedwire** и **Automated Clearing House** (АЦХ). Банке користе Fedwire систем за трансфер средстава на рачуне банака и клијената банака АЦХ систем се користи за трансфер релативно мањих износа. АЦХ плаћања трају дуже у процесуирању и закључивању.

5.2 Fedwire

Fedwire је онлине комуникациона мрежа којом руководи Систем Федералних Резерви која суочава новчане трансфере између финансијских институција. Fedwire се примарно користи за пренос високих новчаних износа. Финансијске институције користе Fedwire за своје кориснике и за закључивање рачуна са другим банкама. Све Fedwire уплате су реализоване. Финансијске институције користе различите методе за приступ Fedwire систему. Систем Федералних Резерви, на пример, нуди мрежу

¹³ Слика 13. Међународна размена [3]

Федлине система, која је уствари софтвер у власништву Федералних резерви за иницирање Fedwire и других форми плаћања. Алтернативно, финансијске институције могу конектовати њихове маинфреаме системе директно на Систем Федералних Резерви за велике трансфере.



14

Слика 14. Fedwire и основне карактеристике [2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

Када корисник на источној обали САД дође у банку и жели да трансферише средства неком другом кориснику на западној обали САД трансакција прелази следећи пут: налог полази из банке и долази до локалног центра где се прослеђује даље ка регионалном центру. Регионални центар препознаје да трансакција треба да се обради у другом регионалном центру и прослеђује је ка централи где се даље рутира трансакција ка свом одредишту. Надаље трансакција се прослеђује регионалном центру на западној обали где се даље рутира ка локалном центру и ка банци која је одредиште трансакције.

5.3. Аутоматед Цлеаринг Хоусе (АЦХ)

Аутоматске клиринг куће су нетинг системи које у неким временским интервалима у току дана обављају мултилатералну компензацију. Све банке које су чланице неке АЦХ током дана достављају своја плаћања ка другим банкама.

5.4. CHIPS (Clearing House Interbank Payments System)

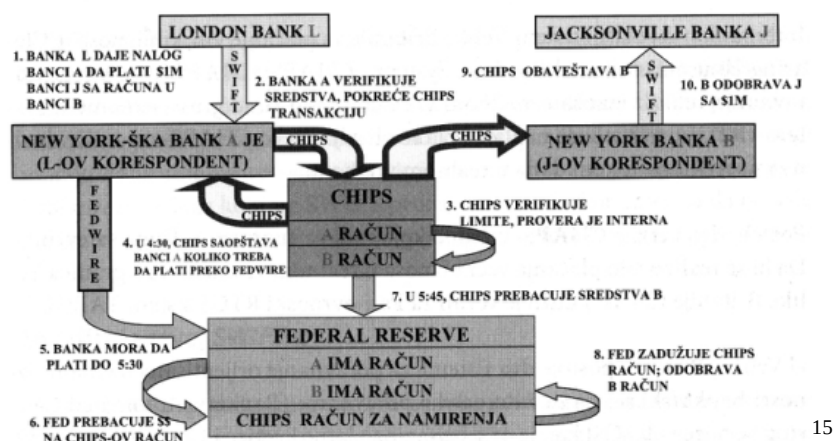
Највећи светски плати систем је Clearing House Interbank Payment System of New York који обавља близу 65 % свих доларских – деноминованих плаћања. CHIPS је приватна институција којом управљају банке чланице. Ради на „неттинг“ систему а финална поравњања се раде преко Fedwire система. Основне карактеристике система:

- ☐ Приватна институција, власник, NY Clearing House Association.

¹⁴ Слика 14. Fedwire и основне карактеристике [2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

- Чланице су 128 банака из 29 земаља.
- Неопозиве трансакције, намирења су на крају дана.
- \$ 1.44Т промета дневно, просечна трансакција \$6.6М
- Цена по трансакцији: \$0.13 - \$0.40



Слика 15. Место Chipsa у процесу плаћања [2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

На слици приказан је поступак провођења међународне трансакције између банке Л и банке Ј. Банка Л започиње трансакцију тако што свом коресподенту банци А шаље SWIFT поруку да са њеног рачуна изврши исплату одређеног износа новца. Банка А која је примила налог даље преузима да спроведе трансакцију. Она мора у том тренутку да има расположива средства и покриће за CHIPS трансакцију. CHIPS прихвата налог да са рачуна банке А пребаци средства на рачун банке Б. Током дана у CHIPS стижу налози за пренос средстава, који потом бивају регистровани и у одређеном тренутку (4x 30` ) CHIPS ради међусобна пребијања и саопштава банци А колико средстава треба да исплати преко Fedwire система. Банка треба у одређеном временском интервалу да изврши плаћање (17x30`) или да изврши рекламацију (ако нешто није сагласно). Банка А преко Fedwire система ради намирење тако што се прво са рачуна А пребаце средства на рачун CHIPS а затим се са рачуна CHIPS пребацују средства на рачун банке Б. Затим банка Б SWIFT-ом обавештава банку Ј да су средства на њеном рачуну у банци Б. Из ове анализе треба сагледати следеће. SWIFT је систем порука, CHIPS је клиринг систем, а Fedwire је систем плаћања.

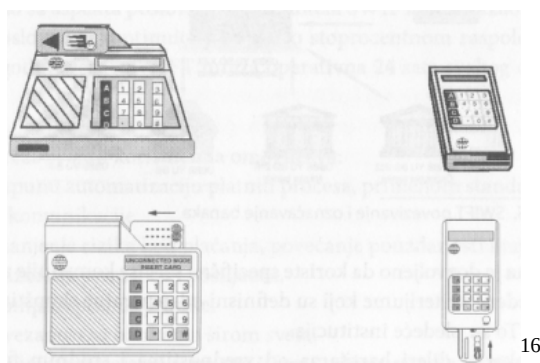
¹⁵ Слика 15. Место Chipsa у процесу плаћања [2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

6.5. SWIFT (Society for Worldwide Interbank Financial Telecommunication)

SWIFT је међународна банкарска мрежа и софтвер за размену података који данас употребљава више од 7000 финансијских институција из 198 земаља. Главни мотив SWIFT-а је да сектору финансијских услуга пружи платформу напредне технологије и приступ заједничким решењима путем којих ће сваки учесник моћи да изгради своју конкурентску позицију на тржишту. SWIFT омогућава размену стандардизованих порука између разнородних финансијских институција тј. банака, берзи, платних система, фондова, клиринг система, а саме поруке се односе на плаћање, трговину, хартије од вредности и остало. Све ове институције морају да испуне захтеве SWIFT критеријуме да би се прикључили једној таквој мрежи. Услуга коју им SWIFT пружа омогућава корисницима сигурност плаћања, снижене трошкове, побољшање аутоматизације и квалитетније управљање ризиком.

Предност коришћење SWIFT-а. Широка распрострањеност и велики број учесника условило је да SWIFT добије примат над осталима телекомуникацијским средствима, тако да су се искристалисале бројне предности коришћења мреже. А то су: предност једноставног приступа разним финансијским институцијама, временски период пријема/креирања порука је максимално скраћен, платформа за креирање порука може се вишеструко користити, широка лепеза услуга по приступачној цени, смањени трошкови преноса порука, побољшан цасхфлов јер информације су ажурне што омогућава боље искоришћавање средстава. Систем заштите. Систем заштите се заснива на комбинацији хардверских и софтверских решења. Стандардна процедура је да када се једна банка укључи у систем, она добија хардверски уређај који представља комуникациони контролер са комплетним системом за криптозаштиту. Уз овај уређај иде и Смарт картица која служи за идентификацију и може се користити само на том уређају. Сваког јутра, на почетку радног дана, оператер покреће процес размене кључева који се користе само тог дана. Сигурност на комуникационим каналима је обезбеђена криптографским механизмима и остварује се кроз више нивоа криптографисања.



Слика 16. Хардверски уређај за заштиту[2]

¹⁶ Слика 16. Хардверски уређај за заштиту[2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

5.5.1. Концепција и организација SWIFT мреже

Систем SWIFT се састоји од различитих системских целина, односно технолошких нивоа мреже, чија хијерархија условљава хардваре, софтвере, комуникациону структуру мреже и међусобне контролне релације и везе. Свака од појединих системских целина спроводи одређени део функција:

Систем Контроле Процеса (System Control Processor)(SCP)

Кришка Процес (Slice Processors)(SP)

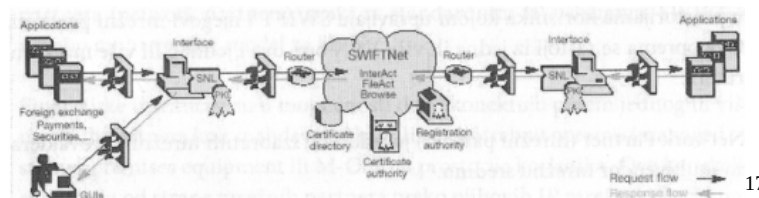
Регионални Процес (Regional Processors) (RP)

SAP

Капија Компјутера (Gateway Computer)

Систем Контроле Процеса (СЦП) се налази у средишту SWIFT система. У оквиру ове мреже постоје два СЦП у УСА и два у Холандији. Међутим, увек је активан само један од њих. Задатак СЦП је да контролише све приступе систему и обавља мониторинг комплетне SWIFT мреже и њихових сервиса, као и дистрибуцију новог софтвера, контролу поновног успостављања везе и стања после прекида у мрежи...

У SWIFT мрежи постоје два Слице процесора од којих је увек активан само један. Слице процесор представља део SWIFT система који комуницира са корисничким логичким терминалом (ЛТ). Задатак СП-а је да усмерава поруке између појединих корисника SWIFT-а преко регионалних процесора, да чува копије свих емитованих порука и на захтев корисника испоставља копију таквих порука, да генерише системске поруке. Сваки Регионал Процесор (РП) логички представља улазну и излазну тачку из SWIFTа. Сви корисници приступају у SWIFT мрежу преко регионалног процесора. Сваку унуту и емитовану поруку проверава регионални процесор, пре него што се упуту на свој даљи пут, према СП. Исто тако и све долазеће поруке се једно време задржавају у одговарајућем регионалном процесору, који спроводи контролу порука, а затим их испоручује на назначену адресу. SWIFT Access Point – САП су мрежни конекциони чворови који подржавају портове кроз које омогућавају корисницима физички приступ SWIFT мрежи. Састоје се од телекомуникационе опреме која је под надзором SWIFT-а са локалном подршком коју обезбеђују локални уговарачи. САП-а има по неколико у земљи, а неке мање земље су прикључене на САП у суседној земљи.



¹⁷ Слика 17. SWIFT [2]

Слика 17. SWIFT [2]

Урош Т., "Електронско пословање", БПШ, Београд, 2005.

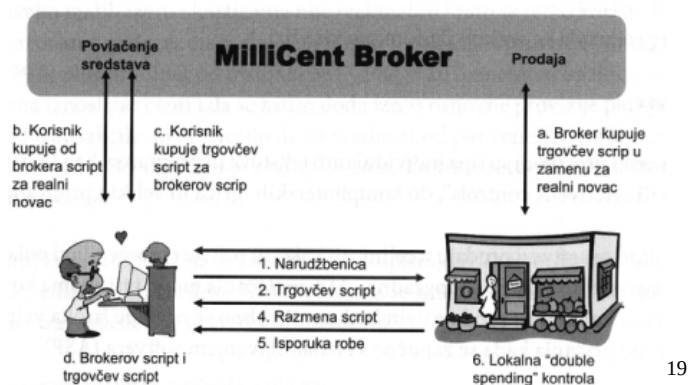
6. МИКРО ПЛАЋАЊА

Врло важан фактор који треба узети у обзир приликом вредновања система за плаћање су додатни трошкови који уносе банкарски сервиси за различите трансакције. У вези са овом идејом појављују се системи за микро плаћање, намењени за обраду великог броја операција преноса малих износа, који таква плаћања у највећем броју случајева групишу ради реализације једне једине трансакције.¹⁸

6.1. Millicent

Millicent је једноставан и сигуран протокол за електронску трговину преко Интернета. Дизајниран је да подржи куповину која кошта мање од цента. базира се на децентрализованом вредности електронског кеша на серверу продавца, без додатне комуникације, скуких шифровања и офф-лине обраде.

Кључну улогу у систему Millicent има брокер и форма електронске валуте названа Script. Брокер води рачуна о: рачуну, наплати, конекцији и успостављању рачуна са продавцем. Script је дигитални кеш који је једино пуноважан код одређеног продавца и пуноважан је за један временски период. Продавац интерно потврђује скрипт да би спречио душло трошење са једног рачуна. Чињеница да би један скрипт одговарао једном продавцу, значи да трговац не мора да контактира брокера да би га потврдио. Ово је значајно јер смањује саобраћај на мрежи и трошкове валидације, пошто брокер делује као посредник. Предност овог система је што се успостављају дуготрајне везе између брокера и купца и брокера и трговца.



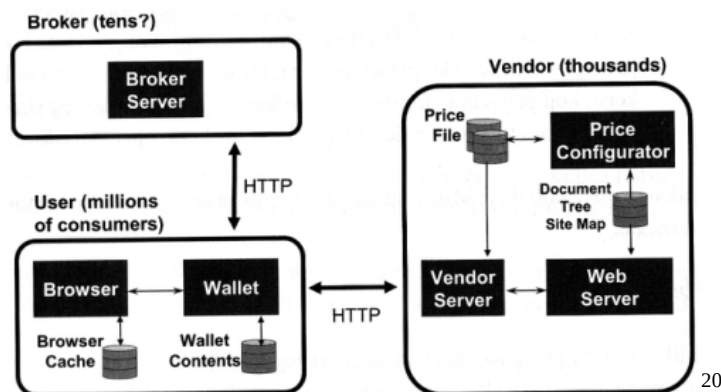
¹⁸ Милан Милосављевић, Владислав Мишковић, "Електронска трговина", Универзитет Сингидунум, Београд, 2011, ст 260. 10.10.3 Микро плаћања

¹⁹ Слика 19. Millicent систем микроплаћања [5]

Слика 19. Millicent систем микроплаћања [5]

Савић А., "Електронско банкарство", Висока ИЦТ, Београд, 2007

Технологија рада је следећа. Трговац ствара специфични – трговачки „Скрипт“ и продаје брокеру за реални новац са попустом. Брокер продаје скриптове од више трговца свим заинтересованим купцима. Скрипт је „препаид“ – обећање купца, да ће их користити за будуће сервисе. Корисници троше scriptove мењајући своје scriptove за скриптове трговца.



Eng/Srb(User(millions of consumers)-Корисник(Milioni korisnika), Wallet- Новчаник, Web Server-Интернет Сервер, Price Configuration- Цена Конфигурације, Vendor Server- Продавчев Сервер, Browser Cache- Претраживач)

Слика 20. Архитектура Millicent система [5]

Савић А., "Електронско банкарство", Висока ИЦТ, Београд, 2007

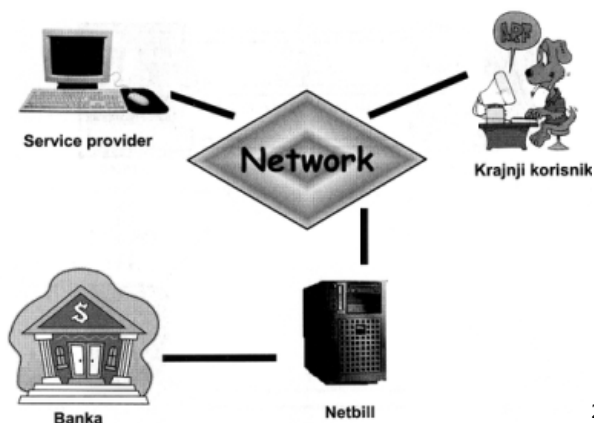
Мале трансакције ограничавају крађу. Мали износи трансакција су на ниском нивоу обезбеђења јер није исплативо да се користи скупа опрема да би се украо јефтин скрипт. Да би се крађом зарадио новац, потребно је да се украде велики број скриптова, али је повећана и могућност да се крађа открије.

Крађа се може детектовати и може јој се ући у траг. Крађа се може приметити нпр. када купац не прими жељену робу. Ако купац вара, губитак за продавца је цена за детектовање неисправног скрипта и одбијање поруџбине. Ако продавац вара, купац пријављује проблем брокеру, који пријављује крађу. Ако брокер вара, продавац ће

приметити неисправне скриптове које прима од тог брокера, и пријавиће крађу. У пракси се показало да је Millicent најпрактичнији за серију малих, нередовних трансакција.

6.2. Netbill

Netbill је систем плаћања развијен на „Carnegie Mellon University“. Користи се као модел плаћања за куповину информационих добра и услуга преко Интернета. Netbill систем ради тако што од купца захтева да има унапред отворен Netbill рачун са кога ће се обавити плаћања. Овај систем плаћања користи симетрични кључ и јавни криптографски кључ. За верификацију се ослања на Керберос систем за криптографију. Netbill трансакција почиње када купац упуту захтев за одређени производ, а завршава се када се прими симетрични кључ за шифрирану робу, која је стигла.



21

Слика 21. Netbill систем плаћања [5]

Савић А., "Електронско банкарство", Висока ИЦТ, Београд, 2007

Концепт Netbilla: на Netbill серверу налазе се оба рачуна, купца и продавца. Ови рачуни су повезани са конвенционалним финансијским институцијама.

Пре него што се активира Netbill протокол, корисник налази информацију која му је потребна на сајту продавца и улази у процес плаћања. Затим се протокол одвија следећим корацима: купац тражи формалну цену од продавца за одређену робу. Продавац, када прими захтев, одређује цену и шаље назад купцу. Ако купцу оговара цена, он шаље инструкције да се изврши наруџбина. Овај процес комуникације се остварује између софтвера купца и продавца. Продавац шаље робу у шифрованој форми до купца. Софтвер на рачунару купца верификује доспеће робе и шаље потписану електронску наруџбеницу до софтвера продавца. Софтвер на рачунару продавца потписује 'чек' и шаље га до Netbill сервера. Netbill верификује цену, суму на чеку и смањује рачун купца за ту суму. такође се чува и копија кључа за дешифровање.

²¹ Слика 21. Netbill систем плаћања [5]

Савић А., "Електронско банкарство", Висока ИЦТ, Београд, 2007

Дигитално потписана наруџбеница враћа се продавцу. Продавац шаље купцу кључ за дешифровање робе. Ако то не учини, кључ се може добити од Netbill сервера.

Netbill делује као агрегатор који комулира мале трансакције у једну велику конвенционалну трансакцију и тако амортизује опште трошкове пословања. Купац и продавац морају да верују Netbill серверу, као трећој страни. Све комуникације које се одвијају на Интернету у оквирима овог система су криптоване. Netbill на страни клијента захтева чековну књижицу (checkbook), док се на страни трговца налазе фиоке за новац (till).

7. МОБИЛНА ПЛАЋАЊА

Конвергенција мобилних комуникација и Интернета отвара нове канале за различите финансијске сервисе. Финансијске институције сада имају могућност да понуде банкарске, брокерске, услуге осигурања преко мобилних телефона, персоналних дигиталних асистената (ПДА). При том оне повећавају лојалност својих клијената као и продуктивност својих запослених.

Када се донесе коначна одлука о преласку на мобилно пословање, велики изазов представља дефинисање успешне стратегије за рад у мобилном окружењу. Успешно пословање у мобилном свету захтева од компанија управо да разумеју разлике између мобилног Интернета и Интернета и да прихвате изазове које пред њих стављају мобилне технологије. Тек тада се може говорити о успеху у свету мобилног пословања. У наставку ће бити речи о кључним захтевима које финансијске институције морају да испуне да би пословали у мобилном свету.

7.1. Мобилни финансијски сервиси

Број финансијских сервиса у великој мери зависи од расположиве мобилне платформе на којој ће се извршавати. Данас имамо различите врсте финансијских сервиса и можемо их поделити на: банкарске, брокерске, сервисе инвестиционог банкарства и друге финансијске сервисе

7.1.1. Банкарски сервиси

Скоро све веће банке су увеле или планирају да лансирају сервисе мобилног банкарства. Док је већина старијих апликација реализована као СМС, двосмерни комуникациони протокол, већина данашњих апликација базирана је на WAP стандарду (Wireless Applications Protocol). WAP омогућава мобилним уређајима да комуницирају преко Интернета једноставним уношењем адресе којој желе да приступе. Ранији сервиси били су типично информационо-базирани, корисници су могли да путем свог мобилног уређаја проверавају стање на рачуну, проверавају стање своје кредитне картице или да добију неке основне финансијске информације. У новијем времену банке су почеле да обједињују могућности трансакција у својим сервисима. Од ових сервиса најчешће се користе плаћање рачуна, пренос средстава или апликације кредитирања.

7.1.2 Брокери

Брокерске куће су хитно неке од својих сервиса пребациле на мобилни Интернет. Независност од времена и локације приступа мобилних брокерских сервиса су веома

атрактивни за оне кориснике који често тргују. Као допуну, мобилни брокерски сервиси нуде својим корисницима да хитро реагују на промене у условима тржишта. Иницијално брокерске куће нису у могућности да понуде сигурне апликације, они су се зато фокусирали на информационо-базиране апликације као што су праћење вести, преглед вредности акција у реалном времену и проверу рачуна.

7.1.3. Инвестиционо Банкарство

Инвестиционе банке су увиделе потенцијал који donosi m-commerce како за повећање продуктивности њихових запослених тако и за додавање нових сервиса за институције и приватне клијенте. Са стране продаје и трговине, инвестиционе банке нуде својим клијентима »Just in case« мобилне апликације које ће у свако доба бити повезане са тржиштем. Важне вести, промене цена, различите анализе могу бити испоручене корисницима одмах по њиховом настајању без обзира на којој се они локацији налазили. Са стране акционарског инвестирања и из области консалтинга, апликације мобилног пословања обезбеђују комплетну финансијску помоћ. Из области консалтинга оне омогућују алате за подршку у одлучивању помоћу којих доносиоци одлука могу да деле своје мишљење са клијентима.

7.2. Принципи пословања мобилног банкарства

Да би у потпуности искористиле предности мобилног пословања, финансијске институције морају дубље разумети кључне стратегије и технологије мобилног тржишта. Основне принципе које финансијске институције морају имати на уму уколико желе да послују у мобилном окружењу су:

Лојалност корисника је важнија од повратка инвестиција –Мобилни Интернет омогућава корисницима да приступе финансијским институцијама са било ког места и у било које време. Из тог разлога, компаније које се баве пружањем финансијских услуга треба да на мобилне сервисе гледају као на дар, а не да брину о томе како ће им се повратити уложене инвестиције. Прихватајући овакав начин рада финансијске институције утичу на повећање лојалности својих корисника тако што им се пружа могућност за праћење животног стила корисника и слично.

Избећи сличност са осталима и у старту понудити различите сервисе, развијајући неке другачије и напредније сервисе, који се не могу наћи било где на тржишту, привлаче се корисници и повећава њихова лојалност. На тај начин може постати лидер на тржишту. Обезбедити иновативне сервисе је значајна шанса за финансијске институције. Они треба да буду различити од опште понуде мобилних финансијских сервиса.

Персонализација је кључ за лојалност корисника - Максимизирање користи од један-на-један природе мобилних уређаја је кључ за успех институција које желе да успоставе јаке везе са корисницима који не зависе од одређене локације.

M commerce мора бити интегрисан са другим корисничким сервисима. Добра m-commerce стратегија не значи да она треба да буде изолована од других корисничких канала у организацији. Компаније које не интегришу своје традиционалне Веб стратегије и Брицк анд Мортал моделе пословања само збуњују и удаљују своје

кориснике. М-цоммерц мора бити инкорпориран у стратегију организације тако да допуњује, и да буде допуњаван од других сервиса. Да ли су апликације прилагођене претходним корисницима. Апликација у мобилном окружењу мора бити бар приближно кориснички орјентисана у тој мери у којој је корисник навикао користећи различите раније услуге компаније.

М-Commerc није само за клијенте – Већина финансијских институција фокусира своју мобилну стратегију ексклузивно на задовољење потреба својих клијената. Овај аспект је наравно веома важан за мобилну стратегију али није неопходно да буде и једини. Запослени такође могу имати користи од мобилних сервиса што доводи до повећања продуктивности и ефикасности. На пример, када инвестициона банка врши истраживања она може имати додатне користи ако најновије информације дистрибуира до својих запослених у тренутку њиховог настајања.

7.2.1. Стратегије мобилног банкарства

Очигледно је да нове технологије стварају нове виртуелне канале за продају и испоруку финансијских сервиса. Мобилни виртуелни канали чак више побољшавају традиционалне банкарске услуге од Интернет канала. Artur D Little идентификовао је три могућа сценарија за излазак на мобилно тржиште.

То су Супер Оператер сценарио, Intimate Seller и Brand Bureau сценарио.

У Супер Оператер сценарију мобилни оператер увећава своје капацитете (мреже, инфраструктуру, број корисника) и проширује своје услуге на улогу агента за плаћање. Банка максималну вредност извлачи из тога што се поставља као стратешки партнер овом доминантном оператеру.

У Intimate Seller сценарију подразумева се да постоји велико хетерогено тражиште где купци покушавају да пронађу жељене производе. Купци у овом случају желе да се обрате на адресу где могу наћи специјалисту за помоћ при обављању трансакције. Банка у Intimate Seller сценарију може наћи могућност за успостављање m-commerce канала.

У Brand Bureau сценарију банка се поставља као институција која ће извршити агрегацију различитих понуда и направити хомогено тржиште за своје кориснике. Банке највише користи могу имати управо у овом сценарију пошто мобилни оператер тада губи предности које је имао у Супер Оператер сценарију где се постављао као доминантан.

Када идентификује најповољнији сценарио банка мора да извуче максимум користи из њега тако што ће развити потребну технологију и испитати потребе тржишта. Банка мора да идентификује значајне partnere које имају сличне циљеве са циљевима банке и успостави сарадњу са њима.

Креира различите портфолије услуга за различите сегменте тржишта. Понудити прави сет услуга на правом тржишту може знатно утицати на повећање броја комитената. На сваком сегменту тржишта треба испитати који су прави, а који потенцијални корисници и које су њихове потребе.

Свим запосленима омогући лак приступ информацијама о корисницима. Информације о клијентима банке углавном су разбацане на више места и налазе се у више

различитих система. Дата мининг техникама омогућити да сви запослени могу лако да добију потребне информације о клијентима.

Пажљиво планира инвестирање у складу са општом стратегијом банке. Успешно лансирање мобилног пословања банке мора бити у складу са општом стратегијом банке. Прелазак банке на нову технологију мора бити јасно дефинисан и усаглашен са дотадашњом информационом инфраструктуром банке.

7.2.2. Техничка инфраструктура мобилног банкарства

1.-Мобилни уређаји

Сваки од мобилних уређаја захтева одређени начин комуникације, они захтевају сопствени gateway за комуникацију са апликативним сервером. Сваки има различиту величину екрана прилагођену различитим врстама приказа података. Различите тастатуре генеришу и различите системе навигације са апликацијом. Изазов за апликативни сервер је да разврстава ове уређаје и да сваком шаље податке у формату који ће бити у складу са њиховим дизајном.

2. Повезивање, Gateway

Полазећи од крајњег корисника, мобилни уређај може бити било који уређај којим он пружа локалном cell centru. Cell center одговара за покривеност одређеног географског региона. Када прими податке он их шаље базној станици. Мобилна мрежа снима и идентификује све потребне информације у локалном регистру, уколико је корисник на локалној географској покривености. Ако није тада станица прати позив, тада се одређује роаминг позива.

3. Бежични средњи слој (апликативни слој)

Апликативни слој је централни део мобилног система. То је место где се ток података контролише, постављају правила, и извршавају фајлови. Апликативни софтвер би требало да буде отворен систем који лако може да успостави комуникацију са другим системима. Један од најчешћих метода комуникације са бацк-енд системима је ХМЛ-АПИ алат за рад са подацима.

7.3. Сигурност

Сигурност је један од најважнијих захтева мобилног банкарства, ако не и најважнији. Истраживања показују да код мобилног банкарства као и код он-лине банкарства корисници имају мало поверења у безбедност апликација. Ефикасан, за сада стандардни начин заштите података на интернету је примена технике јавних кључева (Public Key Cryptography) ПКИ, у основи обухвата приватни и јавни кључ који између себе деле учесници у комуникацији. Трећи елемент, дигитални сертификат, је потписан од треће стране која је ауторизована за издавање сертификата.

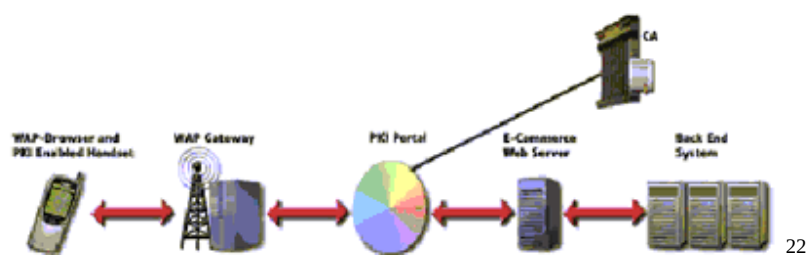
Приказан је поступак рада са трансакцијама базираним на ПКИ технологији:

Пошиљалац криптује своје поверљиве податке помоћу јавног кључа прималаца, битна напомена је да се тајни кључ никад не преноси путем Интернета за време трансакције.

Прималац поруке користи свој тајни кључ који му омогућује да прочита криптовану поруку. Порука може садржати финансијска упутства или друге поверљиве информације.

Уколико неко пресретне поруку он неће моћи да је прочита пошто се она може дешифровати само помоћу тајног кључа који се налази код прималаца.

Да би се осигурали да порука неће бити мењана у току преноса она може да се дигитално потпише. Дигиталан потпис осигурава да подаци нису мењани у току преноса пошто је он везан за податке и свака промена на њима би се открила.



Слика 22. ПКИ технологија [7]

Интернет: <http://www.vps.ns.ac.rs>

Овакав метод заштите драстично смањује могућности за хакерске упаде и повреду сигурности трансакције. Енкрипција заправо представља трговину између безбедности и брзине извршавања трансакција. Брзина криптовања зависи од мобилног уређаја, уобичајено је да се врши са 32-битним процесорима.

7.4. Пример мобилне банкинг апликације

Апликација омогућује да корисници имају увид у своје финансијско стање, а такође су испуњени циљеви које је компанија себи поставила а то су: да систем може да подржава већину трансакција 24 сата дневно, седам дана у недељи, да је сервис спреман да прихвати све већи број потенцијалних корисника без додатног рада на развоју апликације. Омогућено је да се процес веома брзо извршава и да корисник у што краће време долази до података упркос већем броју слојева кроз које они пролазе, и флексибилност – раздвојени су подаци, пословна логика и презентациони слој тако да се лако могу додавати нова решења у систем без потребе за исправкама.

Апликација омогућава кориснику да преко свог мобилног уређаја погледа нову курсну листу, изврши конверзију жељене валуте или погледа стање на свом жиро

²² Слика 22. ПКИ технологија [7]

Интернет: <http://www.vps.ns.ac.rs>

рачуна. Уколико жели да погледа стање на свом жиро рачуну корисник прво мора да изврши идентификацију тако што уноси свој идентификациони број и лозинку.



Слика 23. Мобилна и банк апликација [7]

Интернет: <http://www.vps.ns.ac.rs>

Уколико је идентификација успешна корисник добија списак својих рачуна. На овај начин апликација је поједностављена, јер корисник не мора да уноси број рачуна преко тастатуре, такође је елиминисана могућност грешке која би настала услед погрешно укупаног броја. Након селектовања рачуна корисник на екрану мобилног уређаја добија увид у стање на том рачуну.



Слика 24. Мобилна и банк апликација [7]

Интернет: <http://www.vps.ns.ac.rs>

8. БЕЗБЕДНОСТ ПОСЛОВАЊА НА ИНТЕРНЕТУ

Развој Интернета почео је у САД у доба хладног рата (1969.год.), са идејом прављења мреже рачунара која би обезбедила комуникацију војних лабораторија, владиних бироа и универзитета. Седамдесете године донеле су неколико веома важних открића која су обележила развој Интернета каквог данас знамо, а потом се догодило и одвајање АРПАНЕТ-а из војног експеримента у јавни истраживачки пројект. Вероватно је најважнији тренутак био 1983. кад је тадашња мрежа прешла са НЦП-а (Network

²³ Слика 23. Мобилна и банк апликација [7]

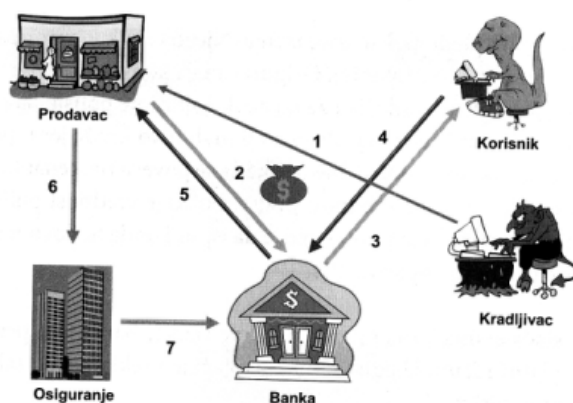
Интернет: <http://www.vps.ns.ac.rs>

²⁴ Слика 24. Мобилна и банк апликација [7]

Интернет: <http://www.vps.ns.ac.rs>

Цонтрол Протокол) на ТСП/ІР (Трансмисион Цонтрол Протокол / Интернет Протокол), што је значило прелазак на технологију каква се и данас користи.

Данас се пословни корисници све више ослањају на Интернет као подршку својим комерцијалним трансакцијама и комуникацији, тако да су интернет провајдери морали да преузму на себе следеће критичне улоге: хостинг за компанијске виртуалне приватне мреже (ВПН), преносници трансакција у електронском пословању, подршка многобројним комерцијалним активностима својих клијената.



25

Слика 25. Процес рекламације [7]

Интернет: <http://www.vps.ns.ac.rs>

Електронска трговина је једно од најчешће нападаних места. Проблем крађа на Интернету може се описати на следећи начин. Крадљивац који дође до података са платне картице легалног корисника долази до сајта трговца и ради регуларну трансакцију са картицом. Трговац, пошто се крадљивац уредно представио, не може да открије да је у питању крађа. Трансакција се уредно извршава и крадљивац добија робу а трговац прослеђује податке на наплату. Трансакција стиже у банку и она такође, није у могућности да открије да је у питању крађа. Банка уредно скида новац са рачуна корисника и обавештава га кроз извод да је трансакција успешно обављена и да је новац скинут са рачуна. Корисник на изводу проналази трансакцију коју није обавио и покреће поступак рекламације. Прослеђује рекламацију банци и она је дужна да по њој поступи. Банка враћа кориснику новац на рачун и пребације новац на рачун сумљивих и спорних потраживања до транутка када се рашчисти ко ће тај износ да плати. Банка обавештава трговца да је урађена нерегуларна трансакција и да трговац разреши овај проблем. Трговац проверава ову трансакцију и констатује да је у питању крађа и пошто је платио осигурање покреће код осигуравајуће компаније поступак накнаде штете. Осигуравајућа компанија проверава да ли је трговац платио полису осигурања и да ли

²⁵ Слика 25. Процес рекламације [7]

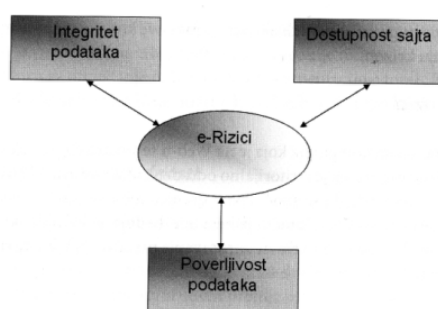
Интернет: <http://www.vps.ns.ac.rs>

су се стекли услови за наплату штете. Ако је све исправно, исплаћује штету трговцу и то пристиже на рачун банке. Тиме је циклус плаћања завршен.

Резултат предходног је следећи: крадљивац је постигао шта је желео, добио је робу али је трансакција оставила траг јер је робу неко морао да преузме на потпис. Његов ризик у овом послу је да буде ухваћен и кажњен за крађу. Трговац је продао робу и платио полису осигурања. Његов ризик је минималан јер је пренет на осигуравајућу компанију. Осигуравајућа компанија преузима ризик крађе зато што је то њена функција и за тај ризик наплаћује полису. Са становишта осигуравајуће компаније добро је да постоји мали ниво крађе јер у противном се нико неби осигуравао. Проблем настаје када се повећа проценат крађе па су онда принуђени да повећају вредност полисе. Пошто је вредност полисе везана са техничким захтевима које трговац мора да испуни онда то доводи и до повећаних инвестиција у технологије заштите.

У оваквим случајевима банка нема никакве ризике. Банци је у принципу све једно ко ће платити рачун. Уједно Банка наплаћује и рекламацију тако да она никада није на губитку. Корисник такође нија на губитку. Покретањем рекламације он је регулисао своју обавезу и има осећај да се окружење брина о његовој сигурности. Ако се крађе понављају и постају учестале, покреће се полицијски поступак. Даља догађања имају следећи сценарио: све се одвија по завршној трансакцији, крађа се открива преко рекламације, неко је преузео робу, на сцену ступа полиција, за овакав поступак мора да постоји законска регулатива.

Са становишта безбедности нека од најбитнијих обележја Интернет пословања на која професионалци из ове области треба да укажу менаџменту у својим фирмама су: иновативни модели пословања, непрекидни и готово неограничени приступ светском глобалном тржишту, усмереност и транспарентност ка клијентима, што за последицу има много бољи и ближи однос, индивидуализација односно прилагођавање купцу (оне то оне), ефикасније пословање и смањивање трошкова уз истовремено низак ниво инвестиција, потреба за јако високим нивоом заштитних мера и сагледавањем нових ризика пословања.



26

Слика 26. Важна обележја Интернета за пословање [1]

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

²⁶ Слика 26. Важна обележја Интернета за пословање [1]

Васковић, В., "Системи плаћања у електронском пословању", ФОН, Београд, 2007.

Ризици пословања на Интернету. Пословње на Интернету креира нови скуп ризика који не покривају највећи број основних пословних полиса осигурања. У ствари, уз ове полисе сада често иде додатак који указује да не осигурава од „он лине“ клеветања или „denial of service“ напада који обарали мреже „е цоммерц“ дивови какви су amazon.com и yahoo.com.

Глобални ризици. По дефиницији свака компанија која је на веб-у се сматра да послује глобално. Већина полиса осигурања је територијално одређена и не покрива од ризика са којима компанија може да се суочи изван границе њихове земље. Највечи број е-commerce осигуравајућих пакета обезбеђује глобално покриће од вируса, хакерских напада, клевета или нарушавања приватности тако да су компаније заштићене без обзира где се штета догодила.

Тестирање безбедности. Суочени са великим ризиција осигуравајуће куће су различите у строгости испитивања сигурности, које оне захтевају, при понуди у висини оштете. Неки желе само тренутни преглед мрежне сигурности, док други долазе месечно да би били сигурни да нису отворене нове рупе на мрежи које би омогућиле лак улаз хакерима. Да би се фирме квалификовале за е-цоммерц, предузеће пролази кроз ригорозну контролу осигуравајуће куће да би се откриле рањивости њиховог електронског пословања. Тестира се такође свест запослених о безбедности укључујући и такозвани социјални инжињеринг.

Социјални инжињеринг. Социјални инжињеринг можемо да посматрамо као „проваљивање запослених“. То у хакерском жаргону значи долажење до информација од људи унутар компаније како би ушли у систем компаније. Зато компаније спровode тестирање запослених да би видели каква је њихова свест о безбедности. Не могуће је да запослени буду потпуно отпорни на преваре и трикове али са одговарајућим тренингом може се драстично смањити број запослених подложних томе.

Анализа организационе безбедности. Почине се од тога да ли компанија има формалну политику о безбедности код запослених или тренинг програме. Препорука је да се сви запослени периодично окупљају по одељењима како би говорили о безбедносним проблемима. Многе компаније то покушавају да одрже кроз електронску пошту али то не доноси неки ефекат. Сваки нови запослени треба да прође тренинг безбедности. Поред основних провера препоручује се детаљнија провера запослених који ће имати приступ поверљивим информацијама фирме. При отпуштању радника потребно је водити рачуна о безбедности. Компаније морају да имају званичну процедуру о отпуштању радника као и званичну документацију о томе. Препоручује се надгледање налога да би се обезбедили од саботаже отпуштених или не задовољних радника.

Анализа техничке безбедности. Ова област укључује интерно и екстерно скенирање мреже компаније. Интерно се проверава да ли су систем и сервери правилно конфигурисани. Проверава се да ли запослени могу да приступе информацијама које иначе не треба да им буде доступно. Највећа интерна сигурносна претња је лош систем лозинки. Запослени често користе исту лозинку за логовање на корпоративску мрежу и за приступ њиховом е-маил систему. Још горе је ако запослени оставе негде записану лозинку где други могу да виде. Екстерна провера тестира компанијски фиревоалс и рутере да виде колико је мрежа сигурна од упада споља, као и да затворе рупе кроз које

би нежељени посетилац могао да прође у случају да је неки порт отворен. Уколико се уоче недостаци компаније добијају одређени рок да исправе недостатке.

Типична покрића. Типична покрића која се нуде на светском тржишту осигурања подразумевају:

Копијутерске преваре и изнуђивање Осигурање компијутерских превара и изнуђивања покрива штету начињену убацивањем вируса у компијутерске системе, злонамерно деловање, неовлашћени трансфер новца на приватне рачуне, коришћење фалсификовање диг. потписа, крађа информација о кредитним картицама као и преваре које проистекну из тога. Оно што у неким случајевима наноси још већу штету од, например, самог изнуђивања, је губитак поверења код клијената, тако да се због тога многи случајеви ни не пријављују.

Штете причињене дигиталној имовини компаније Осигурање од штете причињене дигиталној имовини компаније пруже заштиту у случају губитка или оштећења података или софтвера сачуваних на компијутерској мрежи осигураника услед упада или покушаја упада у мрежу или ширења компијутерских вируса. Признају се трошкови са циљем поновног враћања, конструисања, куповине или прикупљању података или софтвера.

Пословни приходи и екстера трошкови Осигурање прихода и екстера трошкова уствари се односи на штету коју провајдери могу имати услед прекида рада. Штете настале услед прекида пословања покривене су уколико су настале упадима односно покушајима упада у компијутерске мреже, ДоС (Дениал оф Сервице) нападима или усред компијутерских вируса. Неке од последица прекида рада су губитак прихода и екстера трошкови потребни за поновно успостављање рада и опоравак система, губитак корисника и партнера, губитак поверења акционара и на крају капиталне вредности компаније.

ЗАКЉУЧАК

Пословање преко електронских канала представља најбржи, најекономичнији и најефикаснији начин обављања банкарског пословања. Интернет банкарство омогућава обављање банкарског пословања 24 сата дневно, 365 дана у години и то директно из куће или из било ког места на свету где постоји компјутер и прикључак за Интернет. Предности оваквог пословања у односу на класично (филијално) банкарство огледају се у временској и просторној неограничености, брзини обављања трансакција, ниској цени и широком асортиману банкарских производа и услуга. И поред евидентних предности које доноси пословање на Интернету, Интернет банкарство има и одређене недостатке, првенствено изражене у виду одсуства сигурности у пословању, законској (не) регулативи, недостатку приватности, отуђености, одбојности према иновацијама и опасности од злоупотребе Интернет банкарства у криминалне сврхе. Банкарско пословање преко електронских канала је феномен новијег датума, који се одвија, бржим или споријим темпом, последњих тридесетак година. Банкарска индустрија је прилично инертна и склона традиционалним и провереним методама па права револуција у области банкарства, тек предстоји.

Банке су Интернет прихватиле као средство за обезбедивање максимално ефикасног система у обављању банкарског пословања. Главни задатак банкарских институција у свету биће да обезбеде што квалитетније, лакше, ефикасније и посебно безбедније обављање банкарског пословања на Интернету. Српске банке ће преваљити дугачак пут, док не изграде сопствене компјутерске системе, способне да омогуће несметано и безбедно обављање Интернет банкарског пословања.

Два основна модела плаћања путем Интернета су cash-like и cseck-like, док су средства плаћања: електронски или дигитални новац, електронски чекови, кредитне картице, шифроване кредитне картице и потврда треће стране. Начини плаћања преко Интернета могу бити комбинацијом телефон-картица, плаћања поузецем, преко жиро-рачуна и плаћања картицама. Системи плаћања су обичним картицама, смарт картицама, микроплаћања. Најчешћи послови банака на Интернету су: приступ и преглед стања на рачунима корисника, евиденција свих трансакција, плаћања, трансфер новца са рачуна на рачун, измена информација, наручивање чекова и контакти. Развој технологије је довео до аутоматизације пословања и на побољшање испоруке финансијских услуга. Првобитно су уведене automatic teller машине (АТМ), затим ЕФТОПС, телебанкинг, он-лине банкарство, смарт картице. За поуздано функционисање електронског пословања од посебног је значаја правна регулација. »Закон о електронском пословању и електронском потпису«, који је у фази доношења код нас, је неопходан предуслов како за правну заснованост електронског пословања, тако и за укључење у међународне организације и токове.

Заштита система у којем се данас масовно одвијају електронске трансакције представља основни предуслов за функционисање рада банака и њихово пружање услуга клијентима путем канала за електронску комуникацију. Развоју начина заштите електронских канала је посвећена велика пажња имајући у виду осетљивост и поверљивост информација, као и њихов критичан утицај на рад банке. Независност времена и места, као и индивидуалност која је понуђена у коришћењу електронских

услуга су један од основних императива експанзије електронских услуга које банка пружа корисницима представљајући једну ноту индивидуалности, где сваки корисник може бити свој лични банкар, располажући својим средствима 24 часа дневно, сам, без обзира на ком се месту налази, и којим се технологијама служи, а то се може реализовати захваљујући флексибилности система који је створен.

ЛИТЕРАТУРА

- [1] Васковић, В., „Системи плаћања у електронском пословању”, ФОН, Београд, 2007.
- [2] Урош Т., „Електронско пословање”, БПШ, Београд, 2005.
- [3] Митровић Н., „Е-банк“ Сингидунум, Београд, 2005.
- [4] Радовановић П., „Перспектива платних система базираних на дигиталном новцу”, Симпозијум: етрговина 2004, Палић
- [5] Савић А., "Електронско банкарство", Висока ИЦТ, Београд, 2007.
- [6] Интернет: <http://www.etrgovina.otg>
- [7] Интернет: <http://www.vps.ns.ac.rs>
- [8] Интернет: <http://www.racunovodja.rs>
- [9] Милан Милосављевић, Владислав Мишковић, „Електронска трговина ”, Универзитет Сингидунум, Београд, 2011.
- [10] Јовановић, М., Ранков, С.: "Примена електронског пословања у управљању сложеним системима", ИСБН 97-86-7038-054-7, ЦОБИСС.СР-ИД 191422220, Издавач ЈП ПТТ Саобраћаја "С 2012