Мр Видоје Спасић,
асистент Правног факултета, Ниш

Савремени системи електронског плаћања

1. Појава и историјски развој новца

Новац као средство плаћања се јавља на прелазу из првобитне заједнице у робовласничко друштво – пре отприлике 10 до 12 хиљада година. Латински класични назив за новац, *pecunia* (од *pecus*: говедо), води порекло из времена када је говедо, у примитивној робној размени, имало функцију натуралног новца. Нарочиту потребу за новцем изазвала је појава приватне својине и друштвене поделе рада. У почетној фази се као општи еквивалент размене појављују различите врсте роба : стока, шкољке, крзна, оружје, платно, жито, пужеви, стаклена зрна итд. Плаћало се у баруту, робовима, костима. Најтежи новац је био камени новац са острва Јап у јужном Пацифику, а најлакши новац од пера са Јужних Хебрида. Етиопљани су вековима плаћали сољу. У Африци се плаћало слоновом длаком, на Фиџију китовим зубима, у Сибиру опеком бојеном чајем, на Соломонским острвима дуваном… У развијенијим цивилизацијама релативно брзо је долазило до промена па је метални новац и то нарочито племенити метали рано потиснуо натурални новац. У идућој фази новац добија одређен облик и величину одн. тежину. Најстарији такви облици јављају се на Криту пре 1500. године у облику златних бикових глава и златних одн. бакрених полуга у облику одеране животињске коже с ознаком тежине. Најзад, у завршној фази развоја у седмом веку јавља се код Лидијаца у Малој Азији ковани новац с ознаком финоће и тежине. Новац је настао из потребе да се уштеди време при трговини стављањем на комад метала који је имао одредјену тежину и квалитет. Везаност за тежину задржала се у именима неких валута до наших дана. Фунта, лира,

рубља у ствари су, *de facto*, ознаке за тежину. Стара грчка драхма у буквалном преводу значи "шака пуна гвоздених ексера". Новчић од чистог злата тежак три и по грама, тзв. "фиорентино", пред крај 13 века постао је интернационална валута *par excellence*.

У Србији је у 13. веку, у Брскову на Тари, искован први српски новац - grossi de Rassa. Рађен је по узору на Млетачки, али је у њему било мање сребра.

Већ у 11 веку у Кини су се појавиле прве папирне новчанице. У време владавине Кублај Кана новчанице су израђиване од дудове коре. На њима је био владарев печат и потпис његовог благајника. У Француској се током осамнаестог века појављује папирнати новац који је тек пред Први светски рат добио функцију и значај који данас има. Прве банке у данашњем смислу појавиле су се тек у 17 веку. Кредитна картица је настала 1938. године на иницијативу нафтних компанија, а у широј примени је од средине педестих година 20-ог века.

Прва права електронска новчана трансакција јавно је обављена између Женеве и Амстердама на првој World Wide Web конференцији у мају 1994. године. Појава Интернета и преношење пословања на овај медиј знатно је проширила могућности за комуникацију. Ако се некада трговало на вашарима и сајмовима, Интернет је постао виртуелни трг светских димензија. Данас, на почетку трећег миленијума, када се информатичка технологија фантастично развила, дигитално окружење захтева нове облике и системе плаћања. У том смислу се све више говори о електронским облицима плаћања у сајберспејсу.

2. Појам, елементи и особености електронског плаћања

Прелазом из постиндустријског у информатичко доба долази до структуралних промена у свим сферама па и до појмовног померања схватања о одређеним моралним, вредносним и другим категоријама. У том смислу, информација као садржај свести постаје најважнији ресурс не само данашње индустрије, већ и друштва уопште. У складу са тим, једно од најважнијих поља примене савремене технологије на реалне и свакодневне друштвене односе је електронско пословање – обављање финансијских трансакција разменом информација електронским путем. Кључни фактори за увођење електронског пословања су развој сигурних и ефикасних електронских система плаћања. Израстање Интернета као глобалне информацијске мреже и медија којим ће се обављати највећи део трансакција само додатно ставља нагласак на сигурност и поузданост. Савремени системи плаћања ослањају се на методе и поступке криптографије у циљу сигурног чувања и преноса информација (нарочито шифровање и електронско-дигитално потписивање докумената).

Електронско пословање је, по дефиницији, свака робно-новчана трансакција која користи информацију размењену електронским путем. Електронско плаћање је посебан део електронске трговине. Шема електронског плаћања укључује три врсте учесника :

- лице која плаћа електронском готовином (у нашим примерима лице А);
- лице коме се плаћа електронским путем (лице Б);
- финансијска мрежа (углавном банка).

Електронски облици плаћања могу се наћи у различитим облицима:

- дигитални чекови;
- дебитне (чековне) картице;
- кредитне картице;
- картице са ускладиштеном (сачуваном) вредношћу;
- електронска готовина;
- остали облици.

Основне карактеристике својствене већини ових система су : приватност, аутентичност и неопозивост - немогућност побијања обављене трансакције. Суштинска ствар код електронских облика плаћања су мере потребне за гарантовање сигурности порука преношених таквим медијима. У таква сигурносна својства, пре свега, спадају:

• ***приватност*** – заштита преношених података од неовлашћеног читања;

• ***идентификација корисника*** – заштита од лажног представљања услед непостојања физичког и визуелног контакта између лица у трансакцији;

• ***интегритет порука*** – пошто порука може бити пресретнута и промењена потребни су механизми за онемогућавање њене промене или за препознавање њене неаутентичности;

• ***немогућност опозивања*** обављене трансакције – обављено плаћање купац не може оповрћи тврдећи да је неко други уместо њега извршио поруџбину.

Задња три својства везана за електронска плаћања називају се ***аутентичност***. Ова својства се постижу коришћењем аутентификацијске инфраструктуре. У том систему приватност се постиже употребом асиметричне криптографије. Аутентичност страна у комуникацији (њихових јавних кључева) остварује се путем јавног сервиса за генерисање, дистрибуцију и чување корисничких кључева под управом сертификацијског ауторитета или агента од поверења, који су одговорни за проверу корисничког идентитета.

Према Међународној банци за обрачун и плаћања концепт електронског новца може се дефинисати као кореспондентни електронским системима складишта јединица монетарних вредности у поседу потрошача који их користи за извршавање плаћања. Ови системи могу бити материјализовани кроз две форме: електронски новчаник (енгл.“stored-value card“, фр. “le porte-monnaie électronique“) и виртуелни новац или електронска готовина (енгл. “digital cash“, фр. “la monnaie virtuelle“).[1)]

1. Идејни творац концепта дигиталног (електронског) новца је David Chaum, оснивач фирме DigiCash. Ипак, аутор модела електронског новца је Shlomo Rosen, један од директора у компанији Citicorp, који је 1995. године развио и патентирао свој амбициозни подухват под називом – електронски монетарни систем (Electronic Monetary Sistem – EMS).

"Електронски новчаник" омогућава вршење плаћања на бази резерве капитала, претходно створене и материјализоване у облику картице, при чему се овај капитал задужује од трговца при свакој куповини. Овај концепт се, у принципу, користи код трговине на мало. У САД постоји три типа електронског новчаника. Као прво ту спада електронски новчаник на сопственом рачуну клијента. То је off-line систем који није везан на мрежу. Ради се о једном најједноставнијем моделу електронског новчаника, који функционише на потпуно независан начин. Трансакције се региструју на карти која се очитава на терминалу трговца.

Други модел представља "електронски новчаник" на централном рачуну, такође невезан за мрежу, дакле off-line систем. Овај систем омогучава задуживање или кредитирање једног рачуна (нарочито банкарског) који централизује заједничке операције.

Трећи систем представља "електронски новчаник" који је повезан са информационом мрежом, чији рачун је по дефиницији централизован и који је прихватљив за коришћење картице за плаћање, односно чековне картице (debit card), на бази текућег рачуна. За разлику од претходног овај систем омогућава приступ банкарској мрежи и нарочито подизање преко аутоматских дистрибутера.

Виртуелни новац кореспондира софтверима који омогућавају извршавање плаћања преко отворених мрежа, нарочито Интернета. У овом случају резерва капитала је претходно створена и стокирана на компјутеру, али није материјализована, па отуда назив виртуелни кеш.

У САД концепт електронског новчаника остао је, ипак, недовољно раширен.[2)] С друге стране, концепт виртуелног новца је знатно распрострањенији, па је сходно томе, на њему засновано неколико система плаћања.[3)]

2. 1. Електронска готовина-дигитални кеш

Најзначајнији облик електронског плаћања који тежи истим карактеристикама које има плаћање "папирнатом" готовином представља електронска готовина (дигитални кеш).[4)] Овај облик облик плаћања карактерише се неким посебним својствима :

- ***анонимност*** плаћања – лице коме се плаћа не може сазнати идентитет лица које плаћа, и обрнуто;

2. Најпознатија специјализована институција која га користи је Mondex.
3. Sistem Digicash, Sistem Cybecash, Netcash, First virtual и Open market.
4. У ужем смислу, производи на бази електронског новца дефинишу се као продукти са "ускладиштеном вредношћу" или "унапред плаћени" производи у којима је евиденција о средствима или "вредности" која је на располагању клијенту смештена на неком електронском уређају клијента. Ову електронску вредност је клијент купио унапред и она се смањује увек када клијент користи овакав уређај. У ширем смислу дефиниција електронског новца обухвата унапред плаћене картице и софтверске производе који користе рачунарске мреже, а који се називају "дигиталним новцем". (Seitz, Juergen; Stickel, Eberhard : "Internet Banking – An Overview", Journal of Internet Banking and Commerce, Vol. 3, No 2., juin 1998.)

- ***непративост*** плаћања – финансијска институција не може утврдити чији је новац коришћен у одређеној трансакцији.

Основни протокол електронског плаћања готовином састоји се из три основне радње:

- ***withdrawal*** - подизање новца из банке (у којем лице А преноси, у електронском облику, део новца са свог рачуна у банци на *картицу)*;
- ***payment*** – плаћање (лице А преноси део новца лицу Б);
- ***deposit*** - депоновање новца у банку (лице Б депонује новац добијен од лица А на свој банкарски рачун).

Овај протокол може бити имплементиран као on-line или off-line, с обзиром на облик везе између банке и лица коме се плаћа. Као и у сваком систему плаћања, и у електронским облицима плаћања постоје сигурносни ризици који могу бити искоришћени у циљу противправног стицања користи. Протоколи уграђени у систем електронске готовине онемогућавају велику већину таквих покушаја, али безбедност ипак није апсолутна. Треба истаћи да постоје два основна начина преваре код електронске готовине, која представљају аналогију код класичне готовине : фалсификовање *новчаница (банкнота), или креирање ваљаних апоена без одговарајућег подизања новца с рачуна и вишеструко трошење исте новчанице, или репликација једне те исте новчанице.*

Електронски пандан новчанице састоји се од бинарне информације – низа битова – чије је копирање једноставно. Да би се ваљаност новчанице могла проверити и доказати користи се метода електронског (дигиталног) потписа. Свака ваљана новчаница носи потпис финансијске институције која ју је издала, а који не може бити фалсификован. Што се тиче проблема вишеструког трошења он се решава правилом да је век трајања једне новчанице *једна трансакција.*

Највећи број криптографских метода употребљених у имплементацији електронске готовине ослањају се на концепт асиметричне криптографије. Треба истаћи да постоје два основна система електронске готовине : on-line и off-line систем. О*n-line* плаћање подразумева постојање сталне комуникацијске везе између лица Б коме се плаћа и банке, а провера ваљаности новчанице обавља се пре испоручивања плаћене робе. С друге стране, *off-line* плаћање подразумева повремену везу између лица Б и банке, па се ваљаност новчаница обавља накнадно, након испоруке робе. Након обављене трансакције серијски број новчанице записује се у базу података банке, па се свака даља новчаница с истим серијским бројем доспела на депозит одбија као фалсификат. On-line системи могу једноставно открити покушај вишеструког трошења једне исте новчанице и омогућити лицу коме се плаћа откривање преваре. Off-line системи омогућавају детекцију вишеструког плаћања истом новчаницом, али тек након што је трансакција обављена. Стога се уводе додатни механизми који откривају идентитет лица које плаћа ако и само ако је иста новчаница употребљена више пута.

2. 1. 1. Протоколи плаћања електронском готовином

Постоји више протокола плаћања електронском готовином. Приказаћемо само протоколе off-line система, пошто су протоколи on-line система поједностављена варијанта претходних и ређе су у употреби. Три су основна протокола плаћања : једноставан протокол плаћања електронском готовином, протокол непративог плаћања електронском готовином и основни протокол плаћања електронском готовином.

Једноставни протокол плаћања електронском готовином

Једноставан протокол плаћања не укључује анонимност плаћања и немогућност праћења трансакција, што су фундаменталне карактеристике електронског плаћања па се на њему нећемо дуже задржавати.

Протокол непративог плаћања електронском готовином

Код овог протокола остварено је својство непративости, али није присутан карактер анонимности плаћања. Овде је неопходно створити механизам који ће онемогућити банци повезивање појединог подизања новчанице с рачуна лица А с депоновањем те исте новчанице на рачун лица Б. Криптографска метода која се користи у ту сврху је тзв. "слепи потпис" (енг. blind signature). У поступку подизања новца с рачуна, лице А мења поруку која треба бити потписана (а порука је сама новчаница, односно еквивалент серијског броја новчанице) коришћењем случајног броја генерисаног на страни корисника. Битно је нагласити да новчаницу не генерише банка, како не би могла сачувати податке о њој и довести је у везу с обављеном трансакцијом приликом депоновања. Та радња се назива прикривање новчанице (енг. blinding a coin) фактором прикривања (енг. blinding factor). Банка потписује прикривену новчаницу, па лице А уклања фактор прикривања и добија ваљану, потписану новчаницу. Банка ће, по пријему новчанице на депоновање, видети њен серијски број, али је неће моћи повезати с одговарајућим подизањем новца с рачуна лица А.

Основни протокол плаћања електронском готовином

Основни протокол плаћања електронском готовином осим својства непративости трансакција укључује и анонимност плаћања. Међутим, треба истаћи да је тешко остварива имплементација потпуне анонимности, па се у практичним имплементацијама протокола плаћања електронском готовином, акценат ставља само на анонимност купца. Али, с анонимношћу купца настаје проблем откривања починиоца преваре (нарочито у off-line системима) и заштите продавца. Као решење уводи се механизам који открива идентитет лица (енг. identifying information) које је извршило плаћање већ коришћеном новчаницом, док се идентитет савесних купаца штити. Свакако за то се користе криптографске методе. У току поступка подизања готовине из банке, купац уз новчаницу укључује и податке о себи, који су прикривени заједно са серијским бројем новчанице, чију веродостојност банка може проверити на новчаници коју потписује. Банка не види те податке, али може закључити јесу ли веродостојни. Подаци су раздвојени

тако да сваки део за себе не одаје никакву информацију, али оба заједно одају идентитет власника новчанице.

У поступку плаћања, купац мора открити део идентификујуће информације трговцу. Новчаница се, заједно с тим делом информација шаље у банку, где се проверава да ли је она већ коришћена. Део информације који се открива је случајан, па је за свако плаћање различит. Уколико купац покуша новчаницу користити више пута, увек ће од њега бити затражен други део информације. Уколико је новчаница коришћена први и једини пут, банка из дела постојећих података не може открити њеног власника.

2. 2. Идентификујуће информације

Идентификујућа информација укључена је уз сваку електронску новчаницу. Њено основно својство је задржавање анонимности савесних корисника електронске готовине, а откривање идентитета превараната. Постоје два основна начина укључивања идентификујуће информације, који се базирају на механизму дељења тајне.

Први начин се зове identity bit strings. Уз сваку новчаницу укључено је н парова низова идентификацијских битова (енг. identity bit strings). Сваки од ових низова генерисан је на следећи начин :

- лице А креира низ знакова који садрже податке потребне за идентификацију;
- низ знакова дели се на два дела коришћењем протокола за дељење тајне (било која половина тајне је неупотребљива без друге половине);
- лице А се обавезује за сваки податак коришћењем bit-commitment протокола (јамчи непроменљивост података без њихова откривања).

Приликом плаћања, лице Б захтева од лица А откривање једне (случајно изабране) половине сваког од н парова идентификујућих низова. Тај низ назива се одабирући низ (енг. selector string). Лице А открива тражене податке (који сами по себи не откривају њен идентитет), а лице Б проверава њихову ваљаност (упоређивањем с вредностима које је лице А приложило).

У поступку полагања новчанице на рачун, лице Б шаље банци новчаницу, идентификујуће податке лица А и одабирући низ. Банка проверава да ли је новчаница већ коришћена. Уколико су одабирући низови исти, све упућује на то да је лице Б покушало преварити банку. Иако једноставна, ова шема је непрактична због велике количине података потребних за чување информација у свакој новчаници.

Други начин укључивања идентификујуће информације назива се доказ без откривања тајне. Криптографски протоколи којима можемо доказати познавање неке тајне, а без њеног откривања користе се у плаћањима електронском готовином за чување идентификујућих информација и њихово откривање. Користе се на следећи начин:

- сваки корисник електронске готовине у банци за сваку новчаницу поседује јавни и тајни кључ (сходно асиметричној криптографији), а чији тајни кључ указује на идентитет особе. Банка је приликом потписивања новчанице у могућности проверити ваљаност идентификујуће информације путем одговарајућег јавног кључа;
- приликом плаћања, уз саму новчаницу налази се и јавни кључ. Купац доказује трговцу поседовање ваљаног тајног кључа који указује на његову идентификацијску информацију.

2. 3. Питања сигурности код електронске готовине

Суштинско питање код електронског плаћања јесте проблем сигурности. У том контексту на прво место долази вишеструка употреба новчаница. Проблем вишеструке употребе новчанице у on-line системима уобичајено се решава коришћењем базе података коришћених новчаница, али не постоји криптографска метода за спречавање вишеструке употребе новчанице у off-line системима. Један од начина минимизације проблема вишеструке употребе новчаница је постављање лимита на вредност појединог плаћања. За спречавање вишеструке употребе новчаница потребно је имплементирати физичку сигурност. То се постиже преко тзв. сигурне картице, која је у стању онемогућити вишеструко плаћање истом новчаницом брисањем или онемогућавањем потрошене новчанице. Она може имати облик ПЦ картице или "паметне картице" ("smart card").

Други, не мање значајан проблем представља сигурност. У сваком систему са снажним ослонцем на криптографију постоји могућност њеног отказивања, било да се ради о грешци у имплементацији криптографских алгоритама или протокола, напретку криптоанализе или услед људског фактора (губитак тајног кључа, провала у систем, уцена и сл.).

2. 4. "Паметна картица" ("smart card")

Један од савремених начина чувања електронске готовине је "паметна картица". Појам "паметна картица" подразумева микрорачунар смештен у кућиште картице стандардних димензија. Микрорачунар је способан размењивати податке са спољним светом, поуздано их чувати или обрађивати на програмирани начин. Подаци су заштићени од неовлашћеног приступа и релативно сигурни од механичког оштећења картице.

"Паметна картица" представља облик знатно савршеније кредитне, односно магнетске картице. У том смислу, слободно можемо рећи да системи базирани на "паметним картицама" представљају не само садашњост већ и будућност картичне технологије. Технологија "паметних картица" пружа велике могућности коришћења у различитим подручјима. С обзиром на начин примене и функцију коју имају "паметне картице" се могу поделити у три основне групе :

- електронски новчаник ("stored-value card") – "паметна картица" за чување електронског новца;

- кредитна картица (“credit card“) темељена на “паметним картицама”;
- чековна картица – електронски чекови (“debit card“) темељени на “паметним картицама”;

Наравно ова основна подела не лимитира поље примене “паметне картице“ и у другим областима, а нарочито за чување личних или медицинских података, за плаћање јавног телефона, јавног превоза и сл.

Најзначајније поље примене “паметних картица” у електронским системима плаћања је имплементација електронске готовине. Код овог метода плаћања електронском готовином мора постојати медиј који чува електронске новчанице, а то су диск рачунара или картица. Електронска новчаница је низ бројева, створен од стране банке издаваоца применом одговарајућих криптографских метода. Треба истаћи да постоји разлика у терминима “електронски новчаник” и “паметна картица“.“Електронски новчаник” је картица са специфичном програмском подршком прилагођеном конкретној примени – чувању електронског новца. У најширем смислу “електронски новчаник” представља средство преноса и чувања електронких новчаница које се користи у било којем систему електронске готовине.

Поред имплементације “електронског новчаника”, “паметне картице” се могу користити у системима плаћања и као кредитне, односно чековне картице. Међутим, треба подвући да се у “електронском новчанику” могу чувати релативно мање суме новца, до испод 100$. Основна карактеристика система темељених на “паметним картицама“ јесте поузданост, па је скоро немогуће нелегално умножавање новчаница или нелегално креирање нових. Сама картица има довољно снажне процесорске могућности да онемогући нелегални приступ подацима без претходне идентификације власника (нпр. ПИН-ом).

3. Врсте система електронских плаћања

Савремене методе електронског плаћања су бројне и разноврсне па су могуће и различите њихове класификације. Генерално, све методе су подељене у две велике групе базиране на пореклу (извору) новца : (1) методе које почивају на кредитној картици и (2) методе које почивају на банкарском рачуну. Постоје и поделе с обзиром на локализацију електронског новца. Најзад, методе су груписане и биће посматране у функцији њихових поступака трансмисије осетљивих информација. Ове последње подељене су у две групе : методе код којих се трансмисија врши преко уписа и методе код којих се трансмисија врши по основу поруџбине.

С обзиром на порекло (извор) електронског новца методе плаћања које нуде различита специјализована предузећа могу имати следеће облике :

- кредитна карта клијента;
- редован банкарски рачун;
- специјални банкарски рачун;

- хард диск (чврст диск) банке;
- хард диск клијента;
- папирни чек;
- паметна картица (“smart card“).

Резимирајући можемо закључити да су методе електронског плаћања базиране на једном од два извора новца :

- кредитна картица и
- банкарски рачун.

3. 1. Методе базиране на кредитној картици

Кредитна картица је данас веома раширен начин плаћања. Постоји више врста картица[5)] и оне су тако везане за навике потрошача да је савремена куповина незамислива без њих. Све употребе кредитних картица, начелно, могу се поделити у две групе : традиционалне методе и савремене форме. Код прве групе пренос информација од значаја за картицу и потрошача врши се класичним начинима : телефоном (обичним или напредним) или електронском поштом (мејлом). Савремене методе резултат су развоја информатичке технологије, а нарочито су везане за скорији развој криптографије. Ове методе користе јединствено Интернет у процесу поруџбине добара или услуга. При том, неке од ових савремених метода омогућавају процес уписивања преко Интернета, док друге захтевају да осетљиве и значајне информације буду достављене другачије. У овој подшеми процес плаћања користи кредитну картицу клијента за реализовање поруџбина. Разлика код појединих подсистема је у физичком месту где су сачуване (конзервиране) информације које се тичу клијента. Ове информације могу бити постављене на следећим местима :

- кредитна картица са клијентом;[6)]
- кредитна картица код неког посредника или банке;[7)]
- кредитна картица на хард диску клијента,[8)]
- кредитна картица на хард диску банке,[9)]
- кредитна картица и "паметна картица" ("smart card").

3. 1. 1. Кредитна картица са клијентом

Код ове методе клијент мора обезбедити све информације које се тичу његове кредитне картице при свакој куповини, јер ни једна од њих није сачувана код посредника. Највећи део потрошача може преферирати да бројеви њихових картица не буду сачувани код посредника да би смањили ризике злоупотреба. Ипак, они морају бити преношени при свакој куповини, тако да при свакој трансмисији

5. Најпознатије су Visa, Master Card, Diners Club International, American express и др.
6. Овакав систем практикују следећа приватна предузећа специјализована за електронска плаћања : Downtown Anywhere, OpenMarket, случај кад клијент није уписан.
7. CARI, Clickshare, First Virtual, NetMarket, OpenMarket, случај кад је клијент уписан.
8. CyberCash
9. GlobelD

фактички постоје ризици од спречавања (заустављања) информација. Да би се такви ризици смањили користе се криптографске методе. Клијент, дакле, бира између презентирања броја кредитне картице при свакој куповини преко Интернета[10] или прихватања да посредник чува његове податке. Код неких предузећа подаци се, ипак, могу пренети и телефоном, факсом или мејлом, док се код других морају стриктно пренети преко Интернета, коришћењем енкрипције (шифровања).

3. 1. 2. Кредитна картица код посредника или банке

Постоји више метода које укључују посредника између потрошача и продавца. Овај посредник или повезана (удружена) банка чува осетљиве информације да би избегао потребу њиховог преношења при свакој куповини. Оне се преносе само једном код уписа потрошача. На даље, сваки пут кад клијент жели реализовати своју поруџбину на сајту трговца он само презентира свој кориснички број и своју лозинку (pasword), да би могао да изабере жељену робу или услугу. Код ове методе ризик задржавања информација је редукован на само једну трансмисију. Нека предузећа захтевају да информације клијената буду пренете једино путем телефона.[11] Друга омогућавају да буду пренете путем Интернета или телефоном,[12] а нека Интернетом, телефоном, факсом или мејлом.[13] Пошто су информације (подаци) задржане код посредника клијент може користити ове методе са било ког места, под условом да располаже потребним софтвером. У сваком случају, да би клијент користио ове методе он мора имати пуно поверење у свог посредника. Код већине метода из ове групе, трговци не виде никада бројеве кредитних картица клијената, пошто посредник преузима новац у њихово име и за њихов рачун, да би га потом депоновао на рачун продавца. Само у једном случају[14], посредник презентира трговцу потребне информације заједно са фактуром.

3. 1. 3. Кредитна картица на хард диску клијента

Код ове методе информације о кредитној картици се држе на хард диску клијента, који је зависан од свог компјутера за вршење куповине. Уколико поседује лап-топ тај проблем се онда не поставља. При свакој куповини специјализовани софтвер обезбеђује слање преко Интернета осетљивих информација, које су смештене на хард диску клијента. Време потребно за реализовање процеса наручивања и фактурисања умањује сваки ризик грешке у манипулацији. Главни ризик везан за овај метод тиче се злоупотребе, при преносу информација или приликом неког другог приступа компјутеру клијента. Разуме се, инфор-

10. Dawntown Anywhere и OpenMarket, када је клијент уписан.
11. CARI и First Virtual.
12. Clickshare и NetMarket.
13. OpenMarket кад је клијент уписан.
14. NetMarket

мације чуване на хард диску морају бити заштићене на исти начин, као и када се трансмисија врши преко Интернета. С друге стране, још један ризик се назире код ове методе, а то је могућност да информације евентуално буду инфициране вирусом. Међутим, код ове методе не постоји ризик од физичке провале материјала клијента. Пошто хард диск клијента само садржи информације које се тичу кредитне картице, провала или злонамерно функционисање овог система неће проузроковати никакав финансијски губитак везан за начин плаћања. Клијент ће морати једноставно реинсталирати софтвер и поново унети информације.[15)]

3. 1. 4. Кредитна картица на хард диску банке

Ова метода користи хард диск банке за чување осетљивих информација клијената. Информације се, дакле, све чувају на истом месту. Ова околност може онеспокојавати клијенте због привлачности добитка за преваранте. Овај начин почива на поузданости банкарског система. Шема функционисања је следећа. Банка врши исплату трансакције узимајући (скидајући) новац са картице клијента и депонујући износ на банкарски рачун трговца. На тај начин, продавац никада не види информације које се тичу кредитне картице клијента. Ова чињеница ствара погодност за клијента, јер елиминише ризик преваре од стране трговца.[16)]

3. 1. 5. Кредитна картица и "паметна картица"

Код ове методе кредитна картица се користи за депоновање електронског новца на "паметној картици".[17)] Информације везане за кредитну картицу клијента се чувају код посредника. Продавци никада не виде те информације пошто се плаћање врши са "паметне картице" на "паметну картицу". Међутим, употреба паметне картице има више слабости и производи одређене проблеме. Први проблем је руковођење-управљање информацијама везаним за кредитну картицу, јер компаније кредитних картица које желе бити само посредници задржавају бројеве кредитних картица клијената. Други проблем, који знатно ограничава употребу технологије паметних картица на Интернету је логистика. Употреба ових картица захтева коришћење посебног материјала (грађе), који још није приступачан и широј јавности, а камо ли да га има у довољној мери у индивидуалним домаћинствима. Такође, клијент мора имати посебан апарат који омогућава кредит/дебит полазећи од његовог компјутера. Дакле, корисник се мора не само лично представити приликом комплетирања уписа, већ имати инсталиран посебан апарат, као и своју личну "паметну картицу". Најзад, слабост ове методе представља и чињеница да клијент мора лично стати пред читач картице, свој или неки други, за извршење жељене трансакције.

15. Хард диск клијента за смештање осетљивих информација користи CyberCash, употребом криптографских кључева приватног/јавног за обезбеђивање сигурности.
16. Ову методу практикује GlobelD.
17. Пример за овакав модел је Mondex.

3. 2. Методе базиране на банкарском рачуну

Код ове групе метода електронског плаћања, у начелу, не постоји разлика између традиционалних и савремених начина плаћања, као код плаћања базираних на кредитној картици. Неке од ових метода допуштају у исто време упис преко Интернета. Собзиром на порекло електронског новца ове методе се деле на :

- редован банкарски рачун;[18)]
- специјални банкарски рачун;[19)]
- банкарски рачун и " паметна картица".

Разлике код појединих од ових метода огледају се у начину коришћења банкарског рачуна клијента. У једном случају електронски новац се чува код исте банке, док је у другим радије депонован на хард диск клијента. Ако се чува код банке, новац може бити сачуван у облику дигиталних информација или комфорно сачуван такав какав је на банкарском рачуну клијента, одакле може бити подигнут у моменту плаћања. Треба истаћи да методе које користе банкарски рачун клијента, генерално, су знатно ригорозније у моменту уписа захтевајући лично присуство клијента, односно поседовање редовног банкарског рачуна код исте банке. Иначе, поступак уписа, углавном, се врши путем Интернета.

3. 2. 1. Редовни банкарски рачун

Постоје три методе електронског плаћања које се заснивају на редовном банкарском рачуну, али се они међусобно разликују у појединостима. Главна предност ових метода је одсуство проблема везаних за козервацију-чување информација са кредитне картице клијента код посредника. Посредник је овлашћен на чување информација о банкарском рачуну. Такође, посредник је кад-кад банка. Данас овакав модел плаћања углавном практикује неколико великих предузећа.[20)]

Код овог система упис може бити извршен у целини преко Интернета, факса или по избору клијента. Ако се врши путем Интернета користи се енкрипција (приватни/јавни кључ), са употребом ПГП и ССЛ сигурносних система. На даље, ради реализовања поруџбине користи се Интернет. И овде клијент није зависан од банке, пошто посредник руководи процесом плаћања. Новац клијента се не конвертује у електронски новац, он је задржан у банци на редовном банкарском рачуну клијента, према уговору између њега и банке.

3. 2. 2. Специјални банкарски рачун

Код овог система клијент се мора лично представити да би извршио обавезну идентификацију код отварања рачуна. Даље, он ће моћи комплетирати свој упис преко Интернета и извршавати све своје новчане трансакције на тај начин. Један-

18. BankNet, NetCheque, Redi-Check.
19. DigiCash
20. BankNet, NetCheque i Redi-Check.

пут када је електронски новац у дигиталној форми на хард диску клијента, он може вршити куповине. Клијент је одговоран за електронски новац смештен на његовом хард диску. Он мора предузети све мере предострожности да би се избегао губитак таквог новца.[21)]

3. 2. 3. Банкарски рачун и "паметна картица"

Извор новца, у овом случају је или кредитна картица или банкарски рачун. Код овог начина увек је присутан карактер анонимности пошто се плаћање врши са "паметне картице" на "паметну картицу". Тако, никаква информација о клијенту не саопштава се трговцу у току трансакције. Међутим, овде је увек присутан, већ поменути, проблем логистике и трошкови који из њега проистичу.[22)]

3. 3. Друге класификације

Системи плаћања обухватају како трансферне системе малих новчаних вредности, које користе предузећа и потрошачи, тако и међубанкарске системе великих новчаних средстава који подупиру национална и интернационална тржишта новца и капитала. Нова електронска средства плаћања у малопродаји, која се испитују или користе на једном броју тржишта обухватају вишенаменске картице које су плаћене унапред, а називају се "електронске торбице" ("electronic purses") или "електронски новчаник" или дословно "картица за акумулирану суму" ("stored-value card") и механизме плаћања акумулираном сумом којима се плаћање обавља путем отворених компјутерских мрежа као што је Интернет. Осим тога, унапред плаћене картице за једнократну употребу, које често користе конвенционалне магнетске "страјп технологије", сасвим су уобичајене, не само у индустријски најразвијенијим земљама већ и шире, и најчешће се користе за телефонске позиве, паркирања и сл.

Постоје мишљења да би дефинитивна и јединствена класификација система електронског плаћања можда била преурањена, имајући у виду динамичан развој технологије. Ипак, још једна класификација система електронског плаћања заслужује пажњу. С обзиром на начин како се реализује плаћање, системи се могу поделити на оне који су базирани на хардверу или картици, где потрошач користи специјализовани хардвер као што је пластична картица са магнетским жигом или компјутерским чипом, и системе базиране на софтверу или мрежи који функционишу путем софтвера уграђеног у стандардни персонални компјутер, који је прикључен на Интернет. Картица или персонални компјутер садржи електронске податке о износу новчаних средстава која се узимају када потрошач покаже уређај у тренутку продаје или када шаље електронску поруку трговцу.

21. Овај метод плаћања користи DigiCash.
22. Систем који користи овај метод назива се Mondex.

Средства плаћања код електронског новца разликују се по својим техничким аспектима од многих традиционалних облика плаћања. Данас постоје два основна начина представљања вредности новчаних средстава акумулираних на уређају за електронски новац : (1) начин "базиран на салду" где се салдо мења са сваком трансакцијом и (2) начин "базиран на новчаницама", где се "електронске новчанице", свака са фиксном вредношћу и јединственим серијским бројем, пребацују са једног апарата на други.

3. 3. 1. Обим (оквир) примене електронског новца

Термин електронски новац се користи у различитим оквирима да опише велику разноврсност система и технологија плаћања. Системи код акумулиране суме ("stored-value") су углавном инструменти за плаћање унапред где се податак о новчаним средствима потрошача чува у његовом компјутеру а количина акумулиране суме се повећава или смањује кад год потрошач користи апарат да обави куповину или неку другу трансакцију. Насупрот томе, системи приступа су типично они који користе стандардни персонални компјутер са одговарајућим софтвером и потрошачу омогућавају приступ конвенционалном плаћању и банкарским средствима и услугама, као што су кредитне картице и електронски новац путем компјутреских мрежа као што је Интернет или путем других телекомуникацијских веза.

Системи на бази акумулиране суме обухватају картице за акумулирану суму или електронске торбице ("electronic purses"), и слична средства која користе компјутерске мреже, а понекад се називају "дигиталним кешом" или неким другим именима. Многи од предложених системи имају атрибуте како система код акумулиране суме тако и оних код приступа. Треба истаћи да степен сигурности не зависи од тога да ли се систем може користити у компјутерској мрежи, већ да ли се његова сигурност базира на специјализованом механизму отпорном на кварове (заједно са самосталним софтвером) или на софтверу инсталираном у стандардном персоналном компјутеру. Стога, ове две категорије могу се означити као системи засновани на картици и системи засновани на софтверу.

3. 3. 2.Техничко представљање новца

Електронски запис суме акумулиране на компјутеру може се радити на један од неколико основних начина. Апарати могу да акумулирају и располажу бројчаним подацима, вршећи трансакције које могу да смање или увећају салдо (системи који се базирају на салду). Или, компјутери могу да чувају електронске новчанице (назване новчићи или кованице) од којих је свака понаособ идентификована серијским бројем и урађена у фиксном непромењивом апоену. У овом моделу базираном на новчаницама трансакције се врше пребацивањем новчаница са једног уређаја на други а салдо новчаних средстава акумулираних на једном уређају тако постаје сума збир апоена свих новчаница у том компјутеру. Трећи могући приступ, за који се каже да је настао укрштањем претходна два, такође је

могућ коришћењем такозваних електронских чекова који су појединачно идентификовани електронским сертификатима у комбинацији са салдом.

3. 3. 3. Преносивост и примена

Системи код акумулираних средстава разликују се у степену до ког учесници могу да изврше неку трансакцију између себе без учешћа иницијатора или неког другог централног ауторитета. Слободни трансфер, где потрошачи, трговци или банке могу да изврше неограничени број преноса између себе, само је теоријски концепт. У свим анализираним системима трансфер је, у суштини, ограничен, иако се степен и типови ограничења разликују од система до система. У већини система, потрошачи могу једино да плаћају трговцима, а трговци могу једино да изврше пребијање тим новцем или да депонују акумулирани салдо путем својих банака.

У неким системима, потрошачи могу директно да плаћају другим потрошачима али, техничке могућности ограничавају ове начине плаћања путем различитих лимита, укључујући и тачно одређен број таквих директних трансфера или ограничени временски период у току којег овакви трансфери могу да се обаве пре него што захтева контакт са иницијатором или централним оператером. У складу са горе наведеним оквиром, следеће карактеристике дефинишу једну или више основних црта одређеног система.

3. 3. 4. Системи базирани на хардверу (картици) и системи базирани на софтверу

Системи базирани на картици дефинисани су као они који потрошачу нуде специјализовани портабл компјутер, који је у ствари картица заснована на типичном интегрисаном колу и садржи микропроцесорски чип ("паметна картица"). Поред оних који користе "паметне картице", системи базирани на картици су направљени тако да обухватају и оне који користе софистицираније електронске компјутерске справе као што су "електронски новчаници" који обављају специјалне функције или имају веће способности за обраду података.

Системи базирани на софтверу, обухватају оне податке који функционишу путем софтвера инсталираног на стандардном компјутеру, као што је стони компјутер или чак и мањи портабл апарат који поседује потрошач и који следи стандардни оперативни систем. Овакви системи су израђени да би се користили за плаћање преко компјутерских мрежа, првенствено Интернета. Међутим, многи системи базирани на картици могу да се користе преко телефонских веза или затворених или отворених компјутерских мрежа, укључујући Интернет. Стога, битна разлика између система базираних на картици и оних базираних на софтверу јесте у коришћењу специјализованог хардвера у системима који се заснивају на картици.

Код електронског плаћања значајну улогу у његовој имплементацији имају тзв. посредници. Системи са само једним посредником не морају да врше рашчишћавање (клиринг) трансакције у циљу свођења међубанкарских обрачу-

на, али би тај клиринг и обрачунавање били неопходни када би се неке друге посредничке институције (дистрибутери и примаоци) користили за дистрибуирање и сакупљање новца у систему. У системима са вишеструким посредницима, број картице или криптографски сертификат идентификују сваког посредника и куповина или поружбина се пребацују тој институцији на обрачун. Такви системи могу рутински да прикупљају информације о трансакцијама у циљу финансијског клиринга што такође може бити корисно за контролу сигурности.

Код неких трансакција електронског новца, трећа страна даје on-line одобрење пре него што се трансакција може извршити, или пре него што трговац да своју робу или услуге потрошачу. У суштини, on-line трансакције захтевају да информације на компјутеру или оне које пружа корисник, буду потврђене податком са централног компјутера или од стране посредника у осигураним централним базама података. За дати систем on-line одобрење се може користити за све трансакције или за само неке врсте, као што су оне које износ дуга убележавају на банкарски рачун. On-line одобрење захтева додатну комуникацију која знатно може да повећа цену и време потребно за трансакцију.

Трансакције у системима електронског новца, било да су базиране на картици или на софтверу врше се путем размене електронских порука између компјутерских апарата према унапред одређеним протоколима. Поруке се могу пренети путем директног електронског контакта, нпр. између "паметне картице" и уређаја за читање те картице, путем метода за бежичну трансмисију или путем телекомуникацијских линија као што су оне које повезују компјутере у Интернет.

Издавање акумулиране суме у систему електронског новца може да се изврши било пре било у тренутку преузимању. У неким системима електронског новца, акумулирана новчана средства, новчанице или чекове креира издавач и дистрибуира или прво посредничким институцијама па тек онда корисницима. У осталим случајевима издавање може да се обави у тренутку кад потрошач отпочне преузимање.

Преузимање картице за акумулирану суму се типично обавља на АТМ-у путем употребе посебно опремљеног телефона. Снабдевачи очекују да ће у будућности за ову сврху бити на располагању персонални читачи "паметне картице" базиране на компјутеру. Уколико се не плате кешом, кредитном картицом или другим средствима, трансакције преузимања су осмишљене тако да резултирају убележавањем дуга у корисников унапред отворени банкарски рачун који је повезан са картицом. У већини система постоји директна веза са издавачем у процесу преузимања, иако on-line методе преузимања у којима завршетак обраде од стране суиздавача долази након што се новчанице преузму. У неким случајевима преузимања су одобрена без покрића (негативан салдо) на компјутеру, убележавањем дуга на банкарском рачуну након извршених трансакција.

Код система базираних на софтверу, преузимање се обавља на сличан начин путем порука које се шаљу између потрошачевог и издавачевог компјутера. У

пракси се из сигурносних разлога тежи да системи базирани на софтверу врше издавање електронских новчаница или чекова са дигиталним потписом. Плаћање издавачу за овакве електронске новчанице врши се путем директног убележавања дуга на рачуну, кредитном картицом или другим уобичајеним методама даљинског плаћања.

Да би обавио куповину коришћењем система базираног на картици, потрошач убацује картицу у трговачки терминал, који добија увид у његову платежну способност. Терминал проверава да ли је салдо на картици довољан да се изврши трансакција, а затим даје инструкције картици да од своје акумулиране суме одбије износ који се исплаћује. Потрошачева картица затим даје инструкције трговчевом терминалу да увећа свој салдо.

Сличан процес би се одвијао код даљинских плаћања путем компјутерске мреже или телефона, али би потрошач требало да поседује додатну опрему за читање картице. У системима који одобравају трансфере другим потрошачима, додатни уређај (као што је новчаник или телефон) би могао да се користи за обављање исте функције између две картице, било директно, или даљински.

4. Основе криптографије

Пошто имплеметација већине савремених система електронског плаћања нужно захтева примену криптографије, изложићемо неке елементарне појмове везане за ову технологију. Етимолошки криптографија значи писање тајним знацима, симболима. Правно-технички криптографија представља поступак транскрипције или превођења јасне и разумљиве информације у информацију неразумљиву за сва лица осим за кореспондентне стране. Основни циљ постојања и практиковања криптографијеје заштита приватности и пословних података. Најзначајније области примене криптографије представљају : шифровање/дешифровање података, дигитални потпис и електронска трговина, односно електронска плаћања.

4. 1. Шифровање – енкрипција

Шифровање се базира на поједностављеној математичкој функцији чији је излаз зависан од два улазна параметра : оригиналне поруке која се шифрује П и кључа K_1.[23)] Да би шифровану поруку друга особа могла користити потребно је спровести обрнути поступак - дешифровање (декрипција). Дешифровање је, пак, математичка функција чији је излаз зависан од два улазна параметра : шифроване поруке Ш и кључа K_2 . Ако се примени прави кључ K_2, као резултат

23. Кључеви су, у ствари, низови алфанумеричких бројева укључени у математички алгоритам, који се користи за шифровање. Само, пак, шифровање значи да је оригинални редослед бинарних бројева, који чине дигитални фајл промењен у нови редослед који представља шифровано дело. Свако ко зна кључ може извршити обрнуту операцију и добити фајл у првобитном-употребљивом формату.

функције добија се оригинална порука. Према односу кључева K_1 и K_2 криптографске системе делимо на симетричне и асиметричне.

4. 1. 1. Симетрични криптосистеми

Главна карактеристика симетричних криптосистема је: $K_1 = K_2$. Две или више особа деле један исти кључ којим и шифрују и дешифрују поруке. Тиме се остварује тзв. сигуран комуникацијски канал између више људи. Главна предност ових система је једноставност и брзина, али има и више мана : код успостављања сигурног канала треба договорити који ће се кључ користити, па га на сигуран начин пренети свим корисницима канала, што може бити велики проблем ако је физичка удаљеност корисника велика.

4. 1. 2. Асиметрични криптосистеми

Асиметрични системи користе два кључа, јавни и тајни. Кључ K_1 називамо тајним кључем познатим само једном лицу. Кључ K_2 називамо јавним кључем, познатим или доступним свим осталим корисницима система. Под системом можемо разумети и Интернет, па се тако теоријски проширује скуп корисника на читав свет.

Предност овог система је у једноставности креирања сигурног комуникацијског канала између два лица, па, дакле, нема ризичне размене кључа као у симетричним криптосистемима. Слабост овог система представља дужина времена потребног за обављање операције шифровања и дешифровања (око 100 пута дуже од симетричних криптосистема).

4. 2. Електронски (дигитални) потпис

Примена електронског плаћања нужно захтева и употребу дигиталних потписа. Овакви потписи могу настати на два начина : коришћењем симетричних или асиметричних криптосистема, односно алгоритама.

Електронски потписи настали коришћењем симетричних алгоритама темеље се на централној институцији јавног карактера која гарантује аутентичност и извор сваког појединог документа. Корисник таквог система дели тајни кључ с централном институцијом којим се заштићује међусобна комуникација. Уколико документ треба предочити другом кориснику система, централна институција ће документу додати своју информацију којом потврђује извор документа, па ће цели нови документ заштитити одговарајућим кључем дељеним с корисником којем је документ намењен. По пријему поруке други корисник система биће уверен да је документ послат од централне институције и да је извор документа корисник система који је наведен од стране централне институције. Овај начин потписивања је компликован и носи одређене проблеме, од којих су највећи везани за смањење ефикасности централне институције услед оптерећености подацима и пословима. Компромитовање сигурности централне институције као последицу може имати потпуни крах система.

Другу групу чине електронски потписи на бази асиметричних алгоритама. Код ове врсте потписа основни протокол је врло једноставан:

- лице које потписује документ врши шифровање документа својим тајним кључем;
- затим шаље потписани документ лицу коме га жели предочити;
- лице које је примило документ проверава потпис дешифровањем документа јавним кључем потписаног лица.

У овом протоколу нема посредника осим у изузетним случајевима. Овакав протокол задовољава основне карактеристике дигиталног потписа:

- потпис је аутентичан (проверава се јавним кључем потписника);
- потпис је некривотворљив (потписивање се врши тајним кључем кога зна само једно лице);
- потпис се не може поново употребити (потпис је део документа и не може се од њега одвојити);
- документ је непроменљив (уколико се промени ма и један бит у документу, више се не може дешифровати коришћењем јавног кључа потписника);
- потпис се не може негирати, односно опозвати, јер само лице која је потписало документ поседује могућност потписивања својим тајним кључем (зна свој тајни кључ). Једини начин кривотворења потписа је вишеструко коришћење истог потписаног документа (енг. resend-attack). Због тога се код потписивањ докумената наводе датум и време самог чина потписа (енг. timestamping).

Постоје и апликације дигиталног потписа у којима увид у садржај документа није пожељан или дозвољен. Стога су развијени алгоритми потписивања докумената без увида, као и с делимичним увидом у садржај. Потпуно слепи потпис не даје никакав увид у садржај потписаног документа. Једино битно у овом начину потписивања је да је неко документ потписао, као и датум и време потписа. Основно својство потпуно слепог потписа је ваљаност. Он може уверити да је порука потписана од стране потписника. Потпис такође има сва остала својства дигиталног потписа. Лице Б не може довести у везу потписани документ са самим чином потписивања.

Потпуно слепи потпис је у већини случајева сувише ризичан, па се тежи осигурати бар делимичан увид у садржај потписаног документа. Најједноставнији начин за остваривање увида у потписани документ је методом "прережи и одабери" (енг. cut-and-choose). Ова метода се може користити код потписивања електронских новчаница од стране банке.

5. Југословенско право и Европска Унија

Европски Парламент и Савет Европске Уније, имајући у виду развој дигиталне технологије и електронске трговине, у циљу хармонизације прописа у реализовању узајамних плаћања, донели су Директиву[24)] која се односи на активности

установа за електронски новац, као и вршење надзора над таквим установама. У смислу ове Директиве електронски новац се сматра као електронски супституту готовине и банкарских новчаница (банкнота) који је стокиран на електронско средство (медијум) такав као "паметна картица" или меморија компјутера и који је генерално намењен за извршавање електронског плаћања у ограниченим износима.

Под установама електронског новца, у смислу Директиве, подразумева се предузеће или свако друго правно лице, као и кредитна институција, које издаје средства плаћања у форми електронског новца. При том, комерцијалне активности установа електронског новца као издаваоца електронског новца су ограничене на пружање финансијских услуга и нефинансијских које су тесно везане за издавање електронског новца, као и стокажу података на електронско средство за рачун других предузећа или јавних институција.

У Директиви се инсистира на наплативости електронског новца, односно његовој замењивости за стварни новац, како би се сачувало поверење његових ималаца и интегритет система електронског плаћања. Ималац (доносилац) електронског новца може, за време његове важности, захтевати од издаваоца да га исплати у номиналној вредности готовине и у банкарским банкнотама – новчаницама, без икаквих додатних трошкова (чл. 3. ст. 1.). Иначе, односи између издаваоца и имаоца електронског новца морају бити јасно регулисани уговором.

Установе електронског новца врше пласирање новца у износу умањеном за количину која је финансијски ангажована кроз електронски новац у оптицају, како не би настали финасијски поремећаји.

Да би систем електронског плаћања могао нормално да функционише потребно је да се заснива на начелима сигурности. У том смислу, од установа за електронско плаћање захтева се увођење режима правилног и мудрог надзора у циљу елиминисања ризика који носи емисија (издавање) електронског новца, која може погодити стабилност финансијског, односно монетарног система. При том верификацију посебних захтева врши надлежна институција.

У извесним случајевима прописаном Директивом надлежни орган може ослободити установу електронског новца од примене свих или појединих одредаба Директиве.

Државе чланице Европске заједнице дужне су да предузму све мере: нормативне, административне и техничке како би могле почети са имплементацијом електронског плаћања најкасније до 27. априла 2002. године. Уз то, после 27. априла 2005. године надлежна Комисија ће поднети Европском Парламенту и Савету извештај о примени Директиве о електронском плаћању у циљу даљег унапређивања регулативе.

Југославија припада групи земаља које још увек нису извршиле структуралне (а ни законодавне) привредне промене. Процес транзиције, односно својинске

24. Директива 2000/46/ЦЕ донета 18. септембра 2000. у Бриселу.

трансформације још увек је на самом почетку, тако да је тржишна привреда, у постојећим односима, тежак и мукотрпан задатак, који нећемо ни лако ни брзо остварити. Но, без обзира на то ми морамо да пратимо савремене трендове у индустријски развијеним (посебно европским) земљама, како би смо могли да им се у догледно и погодно време, на одговарајући начин прикључимо. На том циљу, као први корак који се намеће, јесте хармонизација легислативе, посебно у области међународне размене добара и услуга где кључну улогу имају плаћања. У том смислу, покренута је иницијатива за доношење Закона о електронском пословању и о дигиталном потпису, чије се усвајање очекује у другој половини 2001. године.

Што се тиче електронског плаћања, Народна банка Југославије донела је Одлуку о начину обављања платног промета електронским путем,[25)] којом је и формално-правно омогућено и уређено безготовинско плаћање између субјеката у платном промету Југославије електронским путем, односно електронским порукама (налозима) преко информационих система. Под електронском поруком сматра се информација која је електронски произведена, потписана дигиталним потписом, послата, проверена, примљена и сачувана електронски (тачка 3. Одлуке). Електронски пренос такве поруке сматра се трансакцијом.

У електронској трансакцији учествују, по правилу, три групе субјеката (тачка 6.). Прву категорију чине тзв. учесници у платном промету који испостављају електронски налог за плаћање или други финансијски документ и могу бити пошиљаоци или примаоци поруке. Другу групу представљају носиоци платног промета, где спадају Народна банка Југославије преко Завода за обрачун и плаћање (Завод), банке, Поштанска штедионица и друге специјализоване финансијске организације које воде рачуне учесника у платном промету (субјеката из прве групе). Најзад, у трећу групу спадају носиоци платног промета – даваоци услуга код електронских трансакција, који су одговорни за прихватање и трансмисију електронских порука између субјеката у електронском промету, као и за друге услуге у складу са уговорима са корисницима. Основни услов за обављање платног промета електронским путем је да сви субјекти располажу компатибилном рачунарско-комуникационом опремом која обезбеђује сигурну и ефикасну комуникацију између субјеката, као и постојање механизама за заштиту података заснованих на дигиталним потписима и дигиталних сертификата које издаје Завод. Уз то, подразумева се да учесници у електронском платном промету морају располагати рачунарском опремом која омогућава електронску обраду података, иначе би електронски промет био незамислив.

Неки субјект може учествовати у електронском платном промету само ако поседује дигитални сертификат на идентификационој картици (ПЛАТИД карти-

25. Одлука је објављена у "Службеном листу" СРЈ бр. 40/2000.

ца), коју издаје Завод. Ова картица служи за безбедно чување тајних кључева на основу којих се креира дигитални потпис њеног власника.

У Одлуци су детаљно уређена права и обавезе свих учесника у електронском промету.

Завод, преко својих организационих делова за клиринг и обрачун, за цертификацију и заштиту, за надзор и управљање обавља следеће послове:

- прима електронске поруке на основу којих се формирају регистри носилаца и правних лица и предузетника и рачуна носилаца и правних лица и предузетника;
- врши пријем налога за међубанкарски клиринг и обрачун од носилаца платног промета и учесника у платном промету и обавља међубанкарски клиринг;
- обезбеђује електронску размену података, врши услуге електронског платног промета преко мреже за повезивање носилаца платног промета (ПЛАТНЕТ мрежа), као и надзор и управљање том мрежом;
- обезбеђује заштиту ПЛАТНЕТ мреже, издаје и опозива дигиталне цертификате за субјекте у електронском платном промету, генерише криптографске кључеве, оверава јавне кључеве и програмира садржај ПЛАТИД картице;
- води регистар издатих и регистар опозваних дигиталних сертификата;
- израђује стандардизовани информациони систем носилаца платног промета (ИСНОПС) за електронску размену порука са Заводом и шаље га носиоцима промета, по непрофитном принципу;

Носилац платног промета – давалац услуга има следеће обавезе :

- спроводи проверу идентификације пошиљаоца;
- проверава аутентичност субјеката који шаље електронску поруку;
- спроводи ауторизацију пошиљаоца, проверавајући обим његових овлашћења;
- проверава интегритет електронске поруке;
- спроводи поступак заштите тајности садржаја електронске поруке;
- проверава послатост и пријем поруке.

Шема електронског плаћања одвија се на следећи начин. Пошиљалац ствара електронску поруку и шаље је електронским путем носицу платног промета – даваоцу услуга који проверава исправност те поруке и електронски је шаље примаоцу. Исправност поруке проверавају, дакле, пошиљалац, прималац и носилац платног промета. Електронска порука која се размењује (која, *de facto*, представља саму трансакцију), мора бити потписана дигиталним потписом на основу тајног кључа који се налази на ПЛАТИД картици. Трансакција је окончана кад крајњи субјект прими поруку.

Поступак заштите се остварује, односно аутентичност пошиљаоца и електронске поруке проверавају, а садржај поруке штити применом криптографских алгоритама, јавних и тајних кључева и дигиталних потписа.

Електронски налог обрачунат у Заводу не може се опозвати. Субјекти у електронском промету су дужни да чувају електронску поруку 10 година након извршене трансакције.

На основу изнетог можемо закључити да Југославија, ипак, колико-толико покушава да прати савремене трендове у области електронског плаћања. У сваком случају остаје обавеза да се предметна материја и законски уреди, чиме би се заокружили нормативни оквири за регулисање електронског плаћања, као интегралног дела електронског пословања које ће бити доминантно у дигиталном окружењу.