Срђан Рајчевић*

УДК 336:347.4

Изворни научни чланак

ЕЛЕКТРОНСКИ ПОТПИС КАО СРЕДСТВО ОБЕЗБЈЕЂЕЊА ПРАВНЕ СИГУРНОСТИ У ЕЛЕКТРОНСКОМ ПОСЛОВАЊУ

doi:10.7168/spm.12.1845.10R

Апстракт

Овај рад за циљ има упознавање са концептом електронског потписа као правног института у оквирима уговорног сегмента електронског пословања, те практичним импликацијама његове примјене, у првом реду повећања степена правне сигурности за уговорне стране. Као технолошка иновација, електронски потпис одликује се сложеним криптографским методама заштите које гарантују аутентификацију, интегритет и непорецивост дигитално потписаних порука. Сходно томе, електронски потпис значајно доприноси ширењу електронске трговине и електронског пословања чинећи га квалитетном алтернативом својеручном потпису и улози коју овај обичај има у уговорном праву.

Кључне ријечи: **електронски потпис, дигитални потпис, електронска трговина, електронско пословање, правна сигурност.**

* Мр Срђан Рајчевић је директор Агенције за информационо друштво Републике Српске

УВОД

Дефиниција појма „потпис", иако као значајна правна радња присутан од зачећа уговорног права, у домаћим и иностраним позитивним прописима ријетко се среће. Оправдање се може пронаћи у поређењу са бројним једнако третираним правним радњама које се убрајају у домен обичаја и које не захтијевају стриктну кодификацију. Међутим, битно је образложити намјену потписа као правног института, а то је манифестација потписникове воље да потписани документ разумије, прихвати као сопствени и да се њиме обавеже или преузме одређена права. Према томе, јасан је значај потписа као правне радње, прије свега, у процесу ступања у правне односе, али и свих других поступака гдје се жели потврдити вјеродостојност садржине писане исправе.

Посебну важност потпис, као метод утврђивања идентитета уговорних страна, добија код географски дисперзованог процеса уговарања, односно уговарања између одсутних страна. Немогућност утврђивања идентитета уговорних страна у оквиру електронског пословања је један од значајних чинилаца који доводе до инвалидације пуноважности тако закључених уговора, првенствено због међународног промета електронских података који постају предмет различитих националних јурисдикција.

У циљу превазилажења ових проблема, у правне системе уведен је институт електронског потписа. Како би он заживио у пракси, захтијева се не само технолошко рјешење, него и ауторитативна правна инфраструктура. Недостатак заједничких материјалноправних упоришта која се односе на технологију електронског потписивања представља додатну препреку за привредне и друге субјекте који би овај систем имплементирали.

Од суштинског је значаја на самом почетку раздвојити појам *електронског* од појма *дигиталног* потписа. Наиме, под широм дефиницијом електронског потписа подразумијевамо „све податке у електронском облику креиране са интенцијом презентације потписа"[1]. С обзиром на овако широку дефиницију, под појам „електронски потпис" можемо

[1] *Information technology professional practice guides*, (eds. Anne-Marie Mooney Cotter), Dublin 2004, 116.

сврстати, нпр. скениран својеручни потпис, потпис на крају поруке електронске поште и сл. Стога је **дигитални потпис**, као технолошка платформа која се базира на асиметричној криптографији која гарантује непорецивост и интегритет електронске поруке од значаја за даљња разматрања у овом раду. Ипак, због раширене употребе термина „електронски потпис", као синонима за потоњу технологију који је своје мјесто пронашао и у називима закона и других правних аката, често се ови појмови користе наизмјеничноу контексту обављања послова **електронске сертификације**.

Постоје два начина за одређивање пуноважности и ефективности дигиталног потписа. Закон може прописати захтијевану форму и истовремено понудити листу прихватљивих форми потписа или његову примјену како би му се дала правна снага. На другој страни, **принцип технолошке недискриминације** одређује употребу дигиталног потписа и признаје му исту правну снагу као и својеручном, притом не правећи било какву разлику у погледу форме. Иако је принцип технолошке недискриминације (еквиваленције) погодан у смислу брзе и ефективне адаптације будућих технолошких рјешења, у поређењу са константним измјенама прописа којима се налаже употреба одређене технологије, његов главни недостатак лежи у чињеници да је могуће признавање пуноважности и нестандардним технолошким методама аутентификације.

Домаћи регулаторни оквир који се тиче дигиталног потписа, а који ћемо представити у наставку, заснован је на принципу технолошке недискриминације. Да би се упустили у правну анализу електронског потписа, предуслов је разматрање технолошког аспекта. Ово из разлога што су електронско потписивање и валидација потписаних докумената у електронском облику фактичке радње које резултирају правном конвалидацијом таквих исправа.

1. ТЕХНОЛОШКИ АСПЕКТ ЕЛЕКТРОНСКОГ ПОТПИСА

Технолошка основа система електронског потписа заснива се на коришћењу криптографије, математичке гране која за циљ има трансформацију података из читљивог у неразумљив облик, као и пратећи

реверзибилни процес. Како би се процес шифровања и дешифровања података успјешно окончао, потребно је коришћење одређених софтверских ентитета, тј. кључева. За разлику од других система заштите (шифровања) електронских података, гдје се за одашиљање и примање порука користи један кључ којим се иста шифрује односно дешифрује (тзв. симетрични криптосистем), систем дигиталног потписа базира се на асиметричној криптографији - процесу у којем се са паром кључева, од којих је један **приватни** и као такав расположив само његовом власнику, а други **јавни** доступан свима, поруке штите од неовлашћеног увида. При томе се шифровање поруке врши јавним кључем, а дешифровање (декрипција) употребом приватног кључа.

Шема дигиталног потписа састоји се од три алгоритма. Први, којем је намјена генерисање кључева, за резултат има постојање пара приватног и комплементарног јавног кључа. Други алгоритам коришћењем приватног кључа креира потпис, док се трећим алгоритмом провјерава оригиналност поруке по основу њеног садржаја, јавног кључа и потписа. Да би овако постављена шема функционисала у пракси, потребно је задовољити два услова: прво, потпис који је заснован на садржају поруке и приватном кључу користи се за провјеру оригиналности употребом одговарајућег јавног кључа и друго, генерисање одговарајућег потписа за страну која не посједује приватни кључ мора бити онемогућено.

Коришћењем дигиталног потписа у електронској комуникацији остварују се три циља. На првом мјесту је аутентификација страна која се постиже везивањем приватног кључа за физичко или правно лице. На другом мјесту је очување интегритета поруке. Наиме, у многим случајевима у којима се захтијева безбједна комуникација, садржај поруке приликом трансмисије не смије бити мијењан. Међутим, иако се криптографским методама садржај може шифрирати на начин да за трећа лица он буде у потпуности неразумљив, садржај шифроване поруке може бити измијењен, а да те чињенице стране учесници у комуникацији не буду свјесне. Дигиталним потписивањем у потпуности се осигурава интегритет поруке, јер свака измјена садржаја за посљедицу има инвалидацију потписа. Коначно, дигиталним потписивањем осигурава се и непорецивост, јер се утврђивањем идентитета стране у комуника-

ције и времена у којем је порука послана, онемогућава порицање одашиљања дигитално потписане поруке.

Проучавањем технолошке поставке система дигиталног потписа намеће се питање потврде аутентичности страна у комуникацији. Јасно је да због насумичног избора страна у комуникацији то није могуће. Како смо претходно установили, предуслов утврђивања идентитета учесника у електронској комуникацији испуњава се јединственим везивањем идентитета физичког лица и приватног кључа. Обје ове компоненте садржане су у тзв. електронском сертификату за чије је издавање задужено треће лице од повјерења односно сертификациони ауторитет. Статус сертификационог ауторитета је, и поред својих техничких одлика и његове непобитно важне улоге у систему електронске сертификације и безбједне комуникације, првенствено предмет правне анализе.

2. ПРАВНИ АСПЕКТ ЕЛЕКТРОНСКОГ ПОТПИСА

Коришћење дигиталног потписа, узевши у обзир његову технолошку поставку и ослањање на криптографију као гарант безбједности, ствара привид супериорности који доприноси подизању степена правне сигурности у електронској комуникацији, а самим тим чини се и изузетно битним у подручјима гдје постоји интерес да степен правне сигурности досегне свој максимум. Конкретно, такав интерес је несумњиво заступљен у процесу закључења уговора у електронском облику, што подразумијева и све радње које закључењу претходе.

Међутим, логична је претпоставка да се идентитет преговарача и будуће уговорне стране може неспорно утврдити и приликом предузимања предуговорних радњи. Коришћење технологије дигиталног потписа по својој технолошкој конструкцији то не обухвата, те се са правног аспекта поставља питање коришћења такве платформе, уколико би она довела до закључења нежељеног уговора или уколико би закључење довело до штетних посљедица. Разумна је претпоставка да би се за рјешавање овог проблема будуће уговорне стране морале обратити и трећем лицу које би уживало њихово повјерење, а све у сврху недвосмисленог утврђивања идентитета. Такво лице морало би да

садржи и електронски сертификат учесника у комуникацији који би био у сваком тренутку доступан на увид.

Ради остваривања правне сигурности приликом слања и прихвата понуде коришћењем технологије дигиталног потписа, уговорне стране користе услуге сертификационог ауторитета (трећег лица од повјерења који своје услуге нуди на комерцијалној или некомерцијалној основи). Сама одредница „ауторитет" подразумијева гаранцију тачности података који се налазе у електронским сертификатима које то тијело садржи, односно јавне кључеве чији су власници лица којима се сертификат издаје. У ту сврху, сертификациони ауторитети подлијежу и материјалноправној одговорности која се односи на нетачност наведених података, или на накнаду штете лицима власницима сертификата уколико се исти на било који начин компромитује.

Субјекти, који се у терминологији појединих законских рјешења називају и *сертификационим тијелима*, у нормативним рјешењима дефинисани су на сљедећи начин:

- „Цертификационо тијело – правно или физичко лице које издаје електронске цертификате или даје друге услуге које су у вези са електронским потписима"[2]
- „Давалац услуга сертификовања подразумијева ентитет или правно или физичко лице које издаје сертификате или пружа друге послове повезане с електронским потписом".[3]

Ипак, ослањањем на услуге сертификационог ауторитета не елиминишу се проблеми који су слични претходно наведеном. Наиме, оправдана је бојазан од лажирања идентитета самог сертификационог ауторитета и у вези са тим налаже се потреба за сертификатом којим се гарантује потврда вјеродостојности његовог дигиталног потписа. У ту сврху најчешће се законима дефинише и сертификациони ауторитет који се налази на врху хијерархијске љествице електронске сертификације. Такав ауторитет обично је одређени државни орган, и за валид-

[2] Закон о електронском потпису Републике Српске, *Службени гласник Републике Српске*, бр. 59/08, чл. 3.

[3] Чл. 2, ст. 11 Европске директиве о електронским потписима

ност његовог дигиталног потписа гарантује сама држава. Дакле, степен правне одговорности који се код крајњих корисника – учесника у кореспонденцији коришћењем технологије дигиталног потписа утврђује снагом врховног сертификационог ауторитета пружа довољну гаранцију за безбједност приликом закључења уговора у електронском облику и систем који се базира на таквој поставци назива се *вертикални систем сертификације*.

Постоје, међутим, случајеви у којима прописи не одређују сертификационо тијело које ће бити врховни ауторитет у хијерархијској поставци електронске сертификације. У таквим конструкцијама, повјерење у рад сертификационог ауторитета и њихова међусобна кореспонденција базирају се на усменом или писменом договору и радној пракси. Овакав систем електронске сертификације назива се и *хоризонтална сертификација*.

С обзиром на то да се сертификациони ауторитети углавном оснивају на комерцијалној основи, законодавци се посебно баве питањем одговорности за насталу штету која се може јавити приликом коришћења њихових производа односно дигиталних сертификата. Неријетко се дешава да се појединi сертификат компромитује или га корисник напросто изгуби, па се у циљу несметане електронске комуникације такви случајеви пријављују ауторитетима који о новонасталим чињеницама обавјештавају јавност, опозивају компромитовани, а у исто вријеме и издају нови сертификат кориснику. Међутим, шта се дешава уколико дође до компромитације самог сертификационог ауторитета односно читаве базе корисничких сертификата?

Закон о електронском потпису Републике Српске обавезама сертификационог ауторитета посвећује читаву главу IV, а такве обавезе између осталог подразумијевају:

- да осигура да сваки квалификовани електронски сертификат садржи све потребне податке у складу са чл. 11. закона,
- да провјери идентитет потписника за кога спроводи услуге сертификације,
- да осигура тачност и цјеловитост података које уноси у евиденцију издатих сертификата,
- да у сваки сертификат унесе основне податке о свом идентитету,

- да омогући сваком заинтересованом лицу увид у идентификационе податке сертификационог тијела и увид у дозволу за издавање квалификованих електронских сертификата,
- да води тачну и заштићену евиденцију електронских сертификата која мора бити јавно доступна,
- да води тачну и заштићену евиденцију неважећих електронских сертификата,
- да осигура видљив податак о тачном датуму и времену (сат и минут) издавања, односно опозива електронских сертификата у евиденцији издатих електронских сертификата,
- да чува све податке и документацију о издатим електронских сертификатима најмање десет година, при чему подаци и пратећа документација могу бити и у електронском облику и
- да примјењује одредбе закона и других прописа којима је уређена заштита личних података.

Материјалноправна одговорност сертификационих ауторитета дефинисана је чл. 40, гдје су прописане новчане казне у случајевима када ауторитет издаје квалификовани електронски сертификат који не садржи све потребне податке дефинисане законом, не спроводи одговарајуће заштитне мјере, не обавијести потписника о свим битним условиме употребе издатог сертификата, не утврди правоваљано идентитет лица коме издаје сертификат, не води безбједно и ажурно евиденцију сертификације и не омогућава њихову јавну доступност, не води ажурну евиденцију опозваних сертификата и друго. Овакво, наизглед круто и са аспекта одговорности строго нормирање обезбјеђује додатни степен повјерења у услуге сертификационих ауторитета од стране корисника.

Поред основне, идентифкационе функције електронског сертификата, исти се може разврставати и по неколико других критеријума. Између осталих, сертификат може бити ауторизујући, односно садржавати и неке друге атрибуте који су специфични у односу на власника као што су старосна доб, пребивалиште, адреса становања и сл. Такође сертификат може бити и трансакциони, чија је особеност одређена подацима који се односе на њихову специфичну улогу у одређеним

трансакцијама, формалностима и сл. Таква врста сертификата садржи и податке битне за ове послове. Поред побројаних, временски сертификат користи се у циљу потврде о постојању одређеног документа у датом тренутку.

Основна категоризација сертификата базира се на њиховој правној снази. Тако се уочава да национална законодавства који су своје прописе доносили усвајајући наднационалне одредбе (што је случај и са Републиком Српском), од којих су најважије оне садржане у Европској директиви о електронским потписима, систем електронске сертификације обрађују у оном дијелу који се односи на *квалификовану електронску сертификацију* и *квалификоване дигиталне потписе*. Како такви дигитални сертификати и потписи подлијежу посебном режиму безбједности и читавом сету услова који се морају испунити да би се њима служило у пословном и правном промету, чини се логичним настојање законодавца да се према овом сегменту електронске сертифкације одреди са пажњом. Стога се садржина квалификованог електронског сертификата, по Директиви, односи на:

- „ознаку да се ради о квалификованом сертификату;
- идентификационом скупу података о даваоцу услуга сертификовања које издаје сертификат и држави у којој је основан;
- имену или псеудониму потписника;
- одредби о укључивању посебног атрибута, односно јединствене карактеристике потписника, уколико је иста релевантна, зависно од сврхе за коју је намијењен сертификат;
- податке за верификацију електронског потписа који одговарају подацима за израду електронског потписа и који су под контролом самог потписника;
- подацима о периоду важења сертификата;
- идентификационој ознаци издатог сертификата;
- напредном електронском потпису даваоца услуга издавања квалификованих сертификата;
- ограничења везаних за коришћење самог квалификованог сертификата, уколико их има;

- ограничења која се односе на вриједност трансакције за које се даје сертификат, уколико их има."[4]

Потребно је, међутим, напоменути да је особеност Директиве, као и њених транспонираних одредби у домаће прописе, и дефиниција затворених (приватних) система електронске сертификације. Унутар таквих система појављују се „обични" неквалификовани сертификати и из њих произашли неквалификовани дигитални потписи за које није потребно претходно испуњавање строгих законских услова у циљу њихове израде и пуштања у промет. Поставља се питање оправданости регулације оваквих дигиталних потписа, иако се њихова примјена често среће у подручјима информационе идентификације и аутентификације, поготово у изолованим информационим системима.

3. ПРЕДНОСТИ И НЕДОСТАЦИ ЕЛЕКТРОНСКОГ ПОТПИСА У КОНТЕКСТУ ЗАКЉУЧЕЊА УГОВОРА У ЕЛЕКТРОНСКОМ ОБЛИКУ

Анализа коришћења технологије дигиталног потписа у контексту закључења уговора у електронском облику намеће потребу утврђивања ефеката примјене такве технологије и омогућавања несметаног и безбједног прометовања путем рачунарских мрежа.[5] На самом почетку потребно је поставити хипотезу – да је дигитални потпис, од свих облика електронског потписа, најквалитетнија замјена својеручном потпису који је присутан приликом закључења уговора у папирном облику.

Да би се ова тврдња оправдала, потребно је извршити детаљну компаративну анализу са примјеном својеручног потписа и утврдити његову намјену. Прије свега, то се односи на саму изјаву воље, тј. исказивање намјере за ступање у правни однос. Сматрамо да је у својству церемонијалне радње, потписивање једнако ефектно и у једном и у

[4] Владимир Савковић, *Правни аспекти електронске трговине*, докторска дисертација, Универзитет Црне Горе, Подгорица 2008, 128.

[5] Као нпр. интернет.

другом случају. Штавише, узевши у обзир комплексност креирања дигиталног потписа употребом криптографских алгоритама и кључа, безбједност дигиталног потписа у смислу евентуалне компромитације (фалсификовања) изразито вишег степена у односу на својеручни, за шта сматрамо да није потребна даљња елаборација.

У погледу доказне функције потписа[6], она се код својеручних потписа утврђује јединственим карактеристикама рукописа сваког потписника, док је код дигиталног потписа она детерминисама приватним кључем којег је практично немогуће фалсификовати, уколико фалсификатор нема приступ бази сертификата унутар сертификационог ауторитета или физички приступ средствима за креирање истог. Напомињемо да и сама садржина документа који се потписује зависи од правилне употребе технологије дигиталног потписа и утолико је могућност њеног кривотворења у потпуности елиминисана, док је код својеручног потписивања папирне документације то чест случај који не изискује посебан напор.

Такође се вриједи осврнути и на саму ефикасност трансакција у смислу брзине цјелокупног процеса закључења уговора. Иако је дигитално потписивање са аспекта коришћења наведених математичких и криптографских метода далеко комплекснији процес у односу на својеручно потписивање, оно се, захваљујући данашњој снази технолошких средстава израде, одвија брже, а исто важи и за пренос дигитално потписаних електронских докумената у односу на класичну кореспонденцију гдје се између одсутних лица размјењују документа у папирном облику.[7]

Даље, битно је истаћи и неке од компаративних предности дигиталног потписа у односу на све друге форме електронског потписа. Снага дигиталног потписа лежи, како смо већ нагласили, у самој технолошкој поставци његове израде, али и објављивања потписниковог сертификата широј јавности. Наиме, да би се сертификат објавио, потребна је регистрација код одговарајућег сертификационог ауторитета, што под-

[6] При томе мислимо на функцију недвосмисленог утврђивања идентитета потписника и потврду вјеродостојности.

[7] Срђан Рајчевић, „Електронска трговина у комунитарном праву", *Аргументи*, бр. 14, 168.

разумијева и претходно закључивање уговора између власника сертификата и лица које се бави пружањем ових услуга. На тај начин, обезбијеђена је претпоставка материјалноправне одговорности и једне и друге стране, што, на крају, гарантује повећан степен правне сигурности у обављању оваквих трансакција.

Основни постулат информационе безбједности детерминисан је тврдњом да је сваки информациони систем или технологија безбједна у оноликој мјери у којој је присутан људски фактор. Чини се да је ова тврдња посебно битна у контексту разматрања конструкције дигиталног потписа као технолошке и правне основе за функционисање правног и пословног промета који се обавља путем рачунарских мрежа. Стога је исправно тврдити да безбједност коришћења дигиталног потписа зависи, прије свега, од опреза и пажње која се посвећује приватном кључу односно његовој физичкој безбједности. Одговарајућим прописима дефинисана је политика безбједног складиштења приватних кључева од стране сертификационих ауторитета, док то није могуће регулисати и за физичка лица односно саме власнике кључева. Тако нису ријетки случајеви компромитације кључева употребом разних малициозних програма и вируса који су присутни на рачунарима крајњих корисника, што представља значајну опасност за безбједност електронских трансакција, а неријетко и стварање негативног публицитета за цјелокупну технологију дигиталног потписа.

ЗАКЉУЧАК

Електронски потпис, а посебно његова правна одредница у виду дигиталног потписа релативно је нов институт нашег правног система. Усвајајући рјешења проистекла из европске правне стечевине, Република Српска начинила је значајне кораке у правцу регулације ове области.

Примарна улога електронског потписа у контексту електронског пословања односи се на утврђивање идентитета уговорних страна, али и на обезбјеђење интегритета саме дигитално потписане поруке, те на непорецивост одашиљања исте. Стога се може констатовати да електронски потпис чини основу уговорног сегмента електронског послов-

ног и правног промета, од чега се значајан дио односи на технолошку конструкцију чијом се комплексношћу омогућавају механизми заштите, истовремено стварајући повјерење између учесника у електронској комуникацији. Кроз системе квалификоване електронске сертификације, државе стварају сопствене правне оквире за обављање ових дјелатности, што адаптацијом униформних законских рјешења резултира стварањем јединственог европског система електронског пословања.

Материјалноправна одговорност сертификационих ауторитета значајно доприноси одабиру технологије електронског потписа у радњама које претходе закључењу уговора, прије свега, због гаранције идентитета сваког потписника понаособ, али и могућности опозива потписниковог сертификата у случајевима отуђења или друге злоупотребе. Сходно томе, стиче се утисак да је улога електронског потписа у предузимању правних радњи путем интернета и ступања у правне односе модерним средствима комуникације од великог значаја, што ће несумњиво допринијети даљњем развоју електронског пословања код нас.

Srđan Rajčević LLM
Director of Agency for Information Society of Republic of Srpska

ELECTRONIC SIGNATURE AS A MEAN FOR ENFORCEMENT OF GREAT LEVEL OF LEGAL SECURITY

Summary

In this article we aim to introduce the reader with the concept of electronic signature as a legal institute which is present in the contracting area of electronic business, as well as its practical implications, primary as a tool that is increasing legal security for contracting parties. As technlogical inovation, electronic signature is characterized by complex cryptographic protection methods that are enabling authentification, integrity and non-repudiation of digitaly signed messages.

Accordingly, electronic signature significantly expands electronic commerce and electronic business, at the same time proving it as quality alternative to handwritten signature and its role in the area of contracting law.

Key words: **electronic signature, digital signature, electronic commerce, electronic business, legal security.**

ЛИТЕРАТУРА

Књиге, чланци

1. В. Савковић, *Правни аспекти електронске трговине*, докторска дисертација, Универзитет Црне Горе, Подгорица 2008, 128.
2. С. Рајчевић, „Електронска трговина у комунитарном праву", *Аргументи*, бр. 14, 168.
3. *Information technology professional practice guides* (eds. Anne-Marie Mooney Cotter), Dublin 2004, 116.

Званична документа

1. Европска директива о електронским потписима 1999/93/ЕС.
2. Закон о електронском потпису Републике Српске, *Службени гласник Републике Српске*, бр. 59/08.