

ЕПИ Търговско право => Авторски публикации => Електронно право и електронна търговия =>
За необходимостта от използването на електронен подпис при електронно банкиране

Тип на документа: авторски материал Актуален към: 28.11.2003 г.	Автор / Източник: <u>Георги Димитров</u> <u>Милка Иванова</u>
Дайджест "Пазар и право", 2003 г., кн. 11	Визирани нормативни актове: <u>Закон за електронния документ и електронния подпис</u> <u>Наредба № 3 от 27.06.2002 г. за безналичните плащания и националната платежна система (отм.)</u>

ЗА НЕОБХОДИМОСТТА ОТ ИЗПОЛЗВАНЕТО НА ЕЛЕКТРОНЕН ПОДПИС ПРИ ЕЛЕКТРОННО БАНКИРАНЕ

Използването на възможностите на информационните технологии е един от ключовите елементи в стратегията на банковите институции, целящи разнообразяване, обогатяване и като следствие от това търсене на предлаганите от тях банкови услуги. Макар и традиционно възприемани като консервативни, за да се наложат на пазара, те непрекъснато създават и предоставят на клиентите си нови типове банкови продукти, един от които са системите за електронно банкиране. Чрез тези системи се осъществява доставката на различни услуги по електронен път, което води до по-ниската себестойност на продукта и позволява достъп до по-голям обхват клиенти. Независимо от предимствата, които предлагат отворените мрежи, и перспективите, които се откриват пред банките участници в търговския обмен, отношенията в тази сфера все още не са свързани със специална нормативна уредба. Това обстоятелство не създава препятствие пред реализирането на концепцията, но поражда множество въпроси, изискващи навременен отговор. Един от тези въпроси е дали масово използваните в съществуващите системи за електронно банкиране средства за индивидуализация на страните и гарантиране на сигурността на транзакцията, като пароли и протоколи за криптиране, са достатъчни, за да удовлетворят нормативните изисквания за подписване на документите и гарантиране на сигурността в оборота.

Направеното по инициатива на IDG през първото тримесечие на 2003 г. анкетно проучване¹ показва, че електронното банкиране се налага като задължителен елемент от услугите на всяка банка. Поради задължението на банката по ЗБ и Наредба № 3 на БНБ за безкасовите плащания и националната платежна система (Наредба № 3)² да предоставя на клиентите определен вид информация, всяка от представените в Интернет банки предлага като минимум извършването на справки за движенията и салдата по сметките. Наред с индивидуалните клиентски справки се предоставя и възможност за реализиране на активни операции такива, при които се извършва отдалечено нареждане на банкова операция от клиента към банката. При осъществяване на последните рядко се предвижда сключване на сделки по електронен път, като договорът за ползване на е-услуги с клиента е в традиционна писмена форма. За момента единствено "Първа инвестиционна банка" АД разчупва тази схема, предлагайки възможност за сключване на сделки *on line*.

От така направения преглед на функциониращите в момента системи за електронно банкиране и информацията, свързана, с тях е видно³, че електронното банкиране е термин, който не се възприема еднозначно в правната и икономическата теория, а при липсата на легална или общоприета дефиниция съдържанието, което се влага в понятието, се характеризира с особено разнообразие. По тази причина преценката относно съществуването на нормативно задължение за използването на електронен подпис по необходимост ще бъде обвързана със съдържанието на понятието "електронно банкиране".

С термина "електронно банкиране" най-често се означава "използването на информационни и комуникационни технологии за улесняване достъпа на клиентите до услугите, предлагани от банката"⁴. Осъществяваната чрез него дейност не попада измежду изброените в закона банкови сделки, но за самата банка предлаганите чрез електронното банкиране услуги имат значението на подпомагащи услуги или се разглеждат като средство за улесняване и стимулиране на търговските сделки по чл. 1, ал. 2 Закона за банките (ЗБ). Съществуващите в момента търговски и банкови отношения в България показват, че е-банкирането традиционно обхваща два елемента: разплащания посредством банкови карти и извършването на услуги, свързани с отдалечено банкиране⁵ чрез използване на персонален компютър, Интернет (WEB) банкиране, телефонно (IVR) или GSM WAP/SMS банкиране⁶. В конкретен случай на Интернет банкирането, макар не безусловно, могат да се обособят две форми: 1) предоставяне на справочна информация за състоянието на сметките и нареждания за плащане, без сключване на банкова или друга сделка по електронен път и 2) виртуален банков клон информационна система за цялостно извършване на една или повече сделки по електронен път⁷.

Имайки предвид преобладаващите видове е-банкови услуги в момента, преценката за съществуването или не на нормативно задължение за използването на електронен подпис ще бъде свързана с преценка на нормативната основа на такова електронно банкиране, при което се осъществяват предимно справочни услуги и се отправят изявления със значение за правото (нареждане на плащания). Настоящото изложение няма да разглежда спецификите на виртуалните банкови клонове и в този смисъл ще разбираме системите за електронно банкиране като "отворен към потребителя уеб интерфейс, чрез който клиентът може да получава специфична за нуждите му информация и да управлява ефективно и удобно парите си".

Въз основа на анализа на законодателството, действащо към началото на октомври 2003 г., може да се направи заключението, че при съставянето на документи, свързани със справочните функции и администрирането чрез системата за електронно банкиране от клиента, нормативно изискване за използване на електронен подпис не съществува. Нещо повече Законът за електронния документ и електронни подпис (ЗЕДЕП) почива на доброволността на използването на електронната форма за размяна на волеизявления между субектите⁸, следователно използването на електронния подпис следва да бъде обусловено от волята на страните.

Не така стоят нещата при платежните документи, доколкото относно извършването на "превод" (активно банкиране) чрез системата следва да се направят следните уточнения. В разглежданите системи договорът между банката и клиента се сключва *off line* и присъствието на клиента е задължително, поради което в конкретния случай под "превод" явно се има предвид не банковата сделка договор за банков превод, а нареждане за плащане по електронен път. Следователно, разглеждайки този въпрос, разбираме банковата операция "превод" като услуга, действие, което представлява попълване на платежно нареждане в електронен вид и неговото изпращане, с което се създава основание за извършването на определено плащане от банката.

Може да се отбележи, че българското законодателство не предвижда забрана за извършването на отдалечено нареждане на банкова операция от клиента към банката, но реализирането на такава дейност следва да се съобрази с някои условия. Член 2, ал. 2 от Наредба № 3 изисква: *"Плащане от банковите сметки да се извършва само по нареждане или с предварително съгласие на титуляра до размера и при условията, поставени от титуляра на сметката или от лицето, откриващо сметката в полза на трето лице титуляр."* На това основание в договора с клиента банката може да уговори даване на съгласие или нареждане в различна форма

(включително по електронен път). Когато е предвидена писмена форма, то поради чл. 3, ал. 2 ЗЕДЕП писмената форма ще се счита спазена, при положение че е съставен електронен документ. Ако конкретното действие изисква "платежен документ" по смисъла на банковото законодателство, то тогава самата Наредба № 3 предвижда възможност за съставянето му в електронна форма в разпоредбата на чл. 12, ал. 4: "Платежните документи могат да се представят на хартиен носител или по електронен път с предвидените в образците реквизити и при спазване **изискванията на Закона за електронния документ и електронния подпис.**" Следователно при активно банкиране платежните документи, съставени в електронна форма в резултат на използването на система за електронно банкиране, следва да съдържат предвидените в образците реквизити и да отговарят на понятието за електронен документ по ЗЕДЕП (а именно: словесно изявление, представено в цифрова форма, чрез общоприет стандарт за преобразуване, представяне и разчитане на информацията, което изявление е записано върху магнитен, оптичен или друг носител и дава възможност да бъде възпроизведено).

За да може нареждането за плащане да обвърже банката, е необходимо то да бъде действително т.е. да бъде съставен такъв платежен документ, който може да послужи като основание за плащане. Когато се касае за услуга, осъществявана посредством система за електронно банкиране, банката трябва да използва система с такива характеристики, които да осигурят валидно изразяване и впоследствие установяване съгласието на автора на изявлението. Наредба № 3 не поставя изискване към вида носител и в този смисъл няма пречка за използване на документ в електронна форма. Наредбата обаче предвижда изисквания към реквизитите на платежните документи, един от които е подписът на наредителя. Поради разпоредбата на чл. 12, ал. 4 от Наредба № 3 изискването платежният документ да бъде подписан със саморъчния подпис на лицето наредител може да бъде удовлетворено с използването на електронен подпис. Съгласно чл. 13, ал. 2 и 3 ЗЕДЕП такъв подпис има значението на саморъчен. Изпълнението на условието за подписване на платежния документ в електронна форма с електронен подпис е необходимо, доколкото не е изрично предвидено в нормативен акт, че натискането на виртуален бутон или друго еквивалентно действие има правното значение на изразена воля⁹. За нуждите на последващото доказване на наличието на подписан електронен документ е препоръчително системата да осигурява функционалност за съхраняване на получените, подписани и изпратени електронни документи в цялост, т.е. документа, заедно с електронния подпис и удостоверението¹⁰.

Изискването за валидно изразяване на воля и възможност за последващото е установяване би могло да бъде спазено тогава, когато продуктът технологично осигурява високо ниво на сигурност, че волята е изразена от титуляра на сметката и че други лица няма да имат достъп до тази възможност. Първият въпрос е свързан с идентификацията на страните в отношението клиент банка, а вторият се определя от сигурността на приложението. Доколкото няма определени конкретни изисквания за информационна сигурност на приложението за е-банкиране, ползвано в отношенията на банката с клиентите, то решаването на този проблем е въпрос на избор на технология и управленско решение във връзка с това.

Вече цитираното проучване на IDG сочи, че осемдесет и девет процента от банките предпочитат идентификационен номер и парола като средство за идентификация на страните в отношението, но само част от тях отдават значение освен това и на криптирането на връзката, чрез използването на SSL или друг вид протокол за криптиране. Поставя се въпросът дали този начин на осигуряване на идентификация на субектите и сигурност на връзката представлява електронен подпис, който съгласно ЗЕДЕП да удовлетвори изискването за подписване на платежен документ.

Сами по себе си нито SSL протоколът, нито паролата или потребителското име

представяват електронен подпис. Последните две осигуряват контрол, ограничаване на достъпа и доколкото лицето поема отговорността да не преотстъпва паролата идентификация на субекта, който ги притежава. SSL протоколът от своя страна е протокол за връзка между частта на системата, която се намира под контрола на клиента (браузъра на клиента), и тази, която е под контрол на банката (банков сървър, приемащ криптирани заявки на клиентите). Този протокол, подобно на останалите протоколи за криптиране, предлага криптиране на информацията на канално ниво. За да можем да говорим за удовлетворяване на изискването за автентичност и интегритет на съобщението (две от функциите на електронния подпис), е необходимо при осъществяване на връзката да бъдат решени три основни проблема 1) клиентът да се увери, че се е свързал със сървъра на банката; 2) данните, които двете страни си обменят, да са неразбираеми за околните и да няма начин трета страна да се намеси в обмена на информация; 3) сървърът да се увери, че с него се е свързал упълномощеният за операцията клиент.

Протоколът за криптиране обаче решава само първите два проблема осигурява ниво на сигурност (интегритета) на предаваните електронни изявления и едностранно по отношение на банката установява факта, че изявленията изхождат от нея като юридическо лице. Последното изискване се изпълнява поради обстоятелството, че за сървъра на банката се издава сертификат за сървър от доставчик на удостоверителни услуги (ДУУ). Когато клиентът се обърне към сървъра, неговият браузър отправя съобщение до LDAP регистъра за публикуваните сертификати на доставчика на удостоверителни услуги, който потвърждава идентичността на сървъра (т.е. на едната от страните в банковата операция). Впоследствие двете страни във връзката си обменят сесиен ключ, който служи за криптиране на данните от предстоящата сесия, но при всяка следваща връзка ключът е различен. Независимо от това, при използването на този протокол няма възможност за установяване кой е насрещният потребител (клиент), защото потребителят влиза анонимно през браузъра, макар и с ПИН идентификация. От друга страна, удостоверението за сървър няма характер на удостоверение за електронен подпис по смисъла на чл. 24 ЗЕДЕП¹¹. Следователно осъществяването на свързаност и размяна на информация за нуждите на е-банкирането по SSL протокол не разкрива самоличността на автора на изявлението *per se* на нито една от двете страни и поради това не може да се приеме за електронен подпис по смисъла на чл. 13, ал. 1 ЗЕДЕП.

Съществуват условия, при реализирането на които използването на SSL протокол за свързаност, комбиниран с идентификация пред системата чрез потребителско име и парола, може да бъде възприет като **обикновен** електронен подпис по смисъла на ЗЕДЕП. Тези условия ще са налице, ако в договора за използване на системата за електронно банкиране страните уговорят следното: 1) че описаният начин за идентификация е достатъчно сигурен за нуждите на отношенията между банката и клиента по договора между тях 2) че криптирането на изявленията със сесиен ключ, извършвано при SSL сесия, ще се разглежда и като подписване и 3) че използването на потребителско име и парола разкрива самоличността на клиента и съгласието му с изявлението.

Дори и при тези условия обаче поради липсата на установена практика при възникването на евентуален съдебен спор банката ще срещне значителни трудности да докаже, че документът е подписан с обикновен електронен подпис. Тези трудности биха били преодолени, в случай че се използва усъвършенстван или универсален електронен подпис, поради създадените от ЗЕДЕП механизми и правни гаранции.

Възможно е да приведем още един аргумент в полза на изложеното становище, че в системите за електронно банкиране е необходимо използването на усъвършенстван

или универсален електронен подпис. Банките са субекти по чл. 3, ал. 2 от Закона за мерките срещу изпиране на пари (ЗМИП) и като такива имат задължението да идентифицират клиента си. ЗМИП въвежда специални изисквания по отношение на "операции и сделки", когато се извършват с електронен документ, електронно изявление или електронен подпис. Следователно е необходимо да се съобразят изискванията на чл. 4, ал. 5 ЗМИП: *"При установяване на трайни търговски отношения или осъществяване на операция или сделка чрез електронно изявление, електронен документ или електронен подпис, или друга форма без присъствието на клиента лицата по чл. 3, ал. 2 и 3 са длъжни да предприемат подходящи мерки за удостоверяване истинността на идентификационните данни на клиента."*

Подходящите мерки *"за удостоверяване истинността на идентификационните данни на клиента"* следва да се преценяват от гледна точка на особеностите на електронната среда, които налагат изискването контактите с клиента да са максимално ограничени и при това от дистанция. Сигурността относно идентификацията на клиента в електронния оборот се осигурява от правните механизми, регламентирани от ЗЕДЕП. Техническа сигурност например се постига посредством създаването на определени законови изисквания за генериране и подписване на електронни документи. ЗЕДЕП въвежда изискването за използване на асиметрична крипто-система, работеща с двойка от частен и публичен ключ, като най-сигурно алгоритмично-техническо решение за постигане на висока степен на сигурност¹². За да се гарантира автентичността и интегритетът на подписаните електронни документи, законът предвижда схема за удостоверяване на притежаването на публичния ключ от точно определено лице посредством издаване на нарочни електронни удостоверения от доверени трети лица доставчици на удостоверителни услуги (ДУУ).¹³

По отношение на правната сигурност със закона се уреждат подробно изискванията към дейността, правата и задълженията на доставчиците на удостоверителни услуги. Разписани са строги правила за издаване на удостоверения, за предоставяне на всяко трето лице на достъп до публикуваните удостоверения и др. В подзаконовите актове по приложение на ЗЕДЕП се конкретизират изискванията към дейността на ДУУ относно: поддържане на разполагаеми средства, които осигуряват възможност за извършване на дейностите в съответствие с изискванията на закона; застраховането им за времето на дейността за вредите от неизпълнение на задълженията; разполагане с техническо и технологично оборудване, което осигурява надеждност на използваните системи; техническа и криптографска сигурност на осъществяваните процеси и т.н.¹⁴

Поради изградената със ЗЕДЕП система за гарантиране сигурността на електронния оборот може да се приеме, че "подходящи" мерки за идентифициране са проверката чрез удостоверението за електронен подпис, издадено от регистриран ДУУ. Аргументи за това отново се откриват в ЗЕДЕП, според който удостоверение се издава, след като ДДУ се увери в истинността на информацията за държателя на ключа и за основанието на представителната власт.

На последно място следва да се обърне внимание върху факта, че електронното банкиране е свързано с размяна на подписана електронна информация. За да се признае на една такава подписана информация качеството на подписан електронен документ, то тя трябва да представлява словесно волеизявление (изразено със средствата на словото), обективизирано в електронна форма, записано на магнитен, оптичен или друг носител, с възможност за последващо възпроизвеждане. Това означава, че за нуждите на електронното банкиране разменяните между банката и клиента подписани електронни документи следва да бъдат в разбираем (словесен) вид и да са подписани с усъвършенстван електронен подпис. Поради тази причина изпращане на подписана с електронен подпис информация извлечение от полетата

на попълнена уеб-форма например, няма да се счита за подписан електронен документ. Макар изпращането и обработването на информация през Интернет да се осъществява точно по този начин, за нуждите на нашия закон няма да се признае качеството на електронен документ. Поради това наред с решенията, предоставящи възможност за обработване, изпращане и съхраняване в бази данни на такава информация, следва да се поддържа успоредна функционалност за подписване и изпращане на четим електронен документ. За същия следва да се осигури съхраняване с оглед възможността за възпроизвеждане в бъдеще.

В заключение можем да обобщим, че при използване на платежни документи (нареждания за плащане) поради предвидените в образците реквизити ползването на електронен подпис е **наложително**. Подходящо е това да бъде усъвършенстван или универсален електронен подпис, доколкото при тях се избягват някои от проблемите, свързани с доказването и стабилността на правните последици от извършената операция. Препоръчително е в системата да се интегрира функционалност за ползване на усъвършенстван (универсален) електронен подпис и по отношение на банката, независимо от използването на протокол за криптиране и съвършен сертификат. В допълнение е необходимо отделно от изпращането на подписана форматирана информация за нуждите на предаването, обработването и съхранението и в бази данни, да се осигури като успоредна функционалност изпращането и получаването на подписаните електронни документи (електронните справки, нареждания и т.н.) да бъде реализирано посредством запазване на тяхната словесна цялост и четимост (plain text), като за целта се използват аплети, подписване на уеб-форми чрез разработени plug-ins и др. подходящи начини.

Георги Димитров, адвокат ОРАК Димитров, Петров и Ко

E-mail: george.dimitrov@orac.bg

Милка Иванова, ОРАК Димитров, Петров и Ко

E-mail: milka.ivanova@orac.bg

1 www.computerworld.bg/events/bf2002/10.04-16_20-16_35-Tania_Hinova-IDG_Bulgaria.ppt

2 ДВ, бр. 75 от 2002 г.

3 Виж Събев, В. Електронното банкиране: задължителен елемент за всяка банка В: сп. Банкови информационни технологии, бр. 1/2003 и представената там статистическа информация.

4 Граматиков, М. В: сп. Банкови информационни технологии, бр. 1/2002, с. 24.

5 Терминът "отдалечено банкиране" често се използва като синоним на електронното банкиране. Произходът му е свързан със специализираната подсистема "Отдалечено банкиране", част от системата за автоматизация на банковата дейност АБанк на А.К.Т.А, разработена още през 1999 г.

6 Прецизността налага да уточним, че GSM WAP/SMS банкирането е термин, свързан с т.нар. м-банкиране (mobile banking), основано на безжични технологии.

Неговото съдържание е по-тясно от понятието е-банкиране.

7 Посочената класификация е базирана на функциониращите системи и е направена за първи път през 2002 г. от М. Граматиков в статия за сп. Банкови информационни технологии.

8 Арг. от чл. 5 ЗЕДЕП.

9 Както например чл. 3, ал. 5 на Наредба № 16 не съвсем прецизно определя, че при картовите разплащания въвеждането на ПИН от клавиатурата представлява електронен подпис.

10 Арг. чл. 3 във връзка с чл. 2 ЗЕДЕП.

11 Удостоверението е електронен документ, издаден и подписан от доставчика на удостоверителни услуги, който съдържа определени реквизити, изброени в чл. 24, ал. 1 ЗЕДЕП в 11 точки.

12 Това изискване обаче касае само усъвършенствания и универсалния електронен подпис.

13 По лекция, изнесена от Г. Димитров на квалификационния курс за адвокати по вътрешни и международни аспекти на търговското право и практика, 18-19 април 2003.

14 Виж Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията за предоставяне на удостоверителни услуги (НДДУУ), Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис (НИАУЕП), Наредба за регистрация на доставчиците на удостоверителни услуги (НРДУУ).
