За необходимостта от използването на електронен подпис при електронно
банкиране

<table>
<thead>
<tr>
<th>Тип на документ: авторски материал</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Автор / Източник:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Георги Димитров</td>
</tr>
<tr>
<td>Милка Иванова</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Дейност &quot;Пазар и право&quot;, 2003 г., кн. 11</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Визирани нормативни актове:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Закон за електронния документ и електронния подпис</td>
</tr>
<tr>
<td>Наредба № 3 от 27.06.2002 г. за безналичните плащания и</td>
</tr>
<tr>
<td>националната платежна система (отм.)</td>
</tr>
</tbody>
</table>

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, целащи 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 осъществяват доставката на различни услуги по електронен път, което води до по-ниская себестойност на продукта и позволява достъп до по-голям обхват на клиенти. Независимо от предприетата, които предлагат отворените мрежи, и перспективите, които се откриват пред банковите участници в търговския обмен, отношенията в тази сфера все още не са свързани със специфична 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 използването в съществуващите системи за електронно банкиране средства за индивидуализация на страните и гарантиране на сигурността на транзакцията, като пароли и протокол за криптиране, са достатъчни, за да удовлетворяват нормативните изисквания за подписване на документите и гарантиране на сигурността в оборота.

Направеното по инициатива на IDG през първото тримесечие на 2003 г. анкетно проучване показа, 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 безактовите плащания и националната платежна система (Наредба № 3) да предоставя на клиентите определен вид информация, всяка от представените в Интернет банки предлагат 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 отделено нараждане на банкова операция от клиента към банката. При осъществяване на последните рядко се предвижда включване на надежно e-услуга с клиентите в традиционна писмена форма. За момента единствено "Първа инвестиционна банка" АД разглежда тази схема, предлагайки възможност за съхраняване на сделки on line.

От така направения преглед на функциониращите в момента системи за електронно банкиране и информацията, свързана, с тях e видно, че електронното банкиране e термин, който не се възприема еднозначно в правната и икономическата теория, а при липсата на легална или обществена 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". Осъществяването 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: разплождана посредством банкови карти и извършването на услуги, свързани с отделенето банкерино чрез използване на персонален компютър, Internet (WEB) банкерино, телефонно (IVR) или GSM WAP/SMS банкерино. В конкретния случай на Интернет банкерието, макар безусловно, могат да се обособят две форми: 1) предоставяне на справочна информация за състоянието на сметките и нараждания за плащане, без спецификация на банковата или друга сделка по електронен път и 2) виртуален банков клон информация система за цялостно извършване на една или повече сделки по електронен път.

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

Въз основа на анализ 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 банкерино от клиента, нормативно изискване за използване на електронен подпис не съществува. Нещо повече Законът за електронния документ и електронен подпис (ЗЕДЕП) почиства на доброволността на използването на електронната форма за размяна на волеизявления между субектите, 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 съдържа 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 нараждане за плащане по електронен път. Следователно, разглеждайки този въпрос, разбираме банковата операция "превод" като услуга, действие, което представлява попълване на платожно нараждане 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 отделено нараждане на банков операция от клиента към банката, но реализирането на такава дейност следва да се обогати с някои условия. Член 2, ал. 2 от Наредба № 3 изисква: "Плащане от банковите сметки да се извършва само по нараждане или с предварително съгласие на титуляр до размера и при условията, поставени от титуляр на сметката или от лицето, откривашо сметката в полза на трето лице титуляр." На това основание в договора с клиента банката може да уговори даване на съгласие или нараждане 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 цифровия формат, чрез общоприет стандарт за преобразуване, представяне и разчитане на информацията, която изявление е записано върху магнитен, оптичен или друг носител и дава възможност да бъде възпроизвеждано).

За да може наредждането 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 изявлениято. 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 платежнияят документ да бъде подписан със саморучния 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 саморучен. 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 устанавяване би могло да бъде спазено тогава, когато продуктът технологично осигурява високо ниво на сигурност, че волята е изразена от титуляря на счетоводната и че други лица няма да имат достъп до тази възможност. Първият въпрос е свързан с идентификацията на страните в отношението на клиент-банка, а вторият се определя от сигурността на приложението. Доколкото няма определени конкретни изисквания за информационна сигурност на приложение за e-банкиране, ползване в отношенията на банката с клиентите, то решаването на този проблем е въпрос на избор на технология и управленичко 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
представляват 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 каналио 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 освеществяване на връзката да бъдат решени три основни проблема: 1) клиентът да се увери, че се е свързал със сървър 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 упълномощения за операцията клиент.

Протоколът за осигурява обаче решава само първите два проблема осигурява ниво на сигурност (интегритета) на предаваните електронни изявлени и едностранино по отношение на банката устанавлива факта, че изявленията изхождат от нея като юридическо лице. Последното изискване се изпълнява поради обстоятелството, че сървърът на банката се издава сертификат за сървър от доставчик на удостоверителни услуги (ДУУ). Когато клиентът се обърне към сървъра, неговият браузър отправя заявка до LDAP регистър за публикувания сертификат на доставчика на удостоверителни услуги, който потвърждава идентичността на сървъра (т.е. единствеността на страните в банковата операция). Впоследствие двете страни във връзката си обменят сесиен ключ, който служи за криптиране на данните от предстоящата сесия, но при всеки следваша връзка ключът е различен. Независимо от това, при използването на този протокол няма възможност за установяване кой е нарешихия потребител (клиент), защото потребителът 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 освеществяването на съвързаност и размяна на информация за нуждите на е-банкирането по SSL протокол не разкрива самоличността на автора на изявлениято през е-видна 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 съвързаност, комбиниран с идентификация пред системата чрез потребителско име и парола, може да бъде възприето 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 като подписване и 3) че използването на потребителското име и парола разкрива самоличността на клиента и съгласието му с изявлениято.

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 създаването 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 "операциите и сделките", 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 трънни търговски отношения или осъществяне 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." Първостепенна значимост имат мерките за удостоверяване на истинността на идентификационните данни на клиента. "За удостоверяване истинността на идентификационните данни на клиента" следва да се преценяват от гледна точка на особеностите на электронната среда, които налагат изискването контакта с клиента да са максимално ограничени и при това от дистанция. Сигурността относно идентификацията на клиента във връзка с електронен обмен се осигурява от правилата, регламентирани от ЗЕДЕП. Техническа сигурност например се постига посредством създаването на определени законови изисквания за генериране и подпълване на електронни документи. ЗЕДЕП въвежда изискването за използване на асиметрично криптосистема, работеща с двойка от частен и публичен ключ, като най-пълно алгоритмично-техническо решение за постигане на висока степен на сигурност. За да се гарантира автентичността и интегритетът на подпълваните електронни документи, законът предвидя схема за удостоверяване на притежаването на публичния ключ от точно определено лице посредством издаване на нарочно електронни удостоверения от доверен трети лица доставчии на удостоверителни услуги (ДУУ). По отношение на правната сигурност със закона се уреждат подробно изискванията към дейността, правата и задълженията на доставчии на удостоверителни услуги. Разпредели се строго правила за издаване на удостоверения, за предоставяне на всеки трето лице на достъп до публикуваният удостоверения и др. В подзаконовите актове по приложение на ЗЕДЕП се конкретизират изискванията към дейността на ДУУ относно: подпълване на разполагаеми средства, които осигуряват възможност за извършване на дейността 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 надежност на използваните системи; техническа и криптографска сигурност на осъществяваните процеси и т.н. Поради изграждането със ЗЕДЕП система за гарантиране сигурността на електронния обем 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 ДУУ се увери в истинността на информацията за държателя на ключа и за основаното на представителната власт. На последно място следва да се обозре внимание върху факта, че електронното банкиране е свързано с размяна на подписана електронна информация. За да се признаяе на една такава подписана информация качеството на подписан електронен документ, то тя трябва да представлява словесно волеизявление (изразено със средствата на словото) обективирано в електронна форма, записано на магнитен, оптичен или друг носител, с възможност за последващо възпроизвеждане. Това означава, че за нуждите на електронното банкиране разменяваните между банката и клиента подписани електронни документи следва да бъдат в разбиране (словесен) вид и да са подписани с усъвършенстван електронен подпис. Посред тази причина изпращане на подписана с електронен подпис информация извънчение 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 е се призная 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 четири електронен документ. За същия случай 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 доказането 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 съврътен сертификат. В допълнение е необходимо отделно от изпращането на подписана информация за нуждите на предаването, обработването и съхранението в база 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 целост 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.


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.н. 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 пример 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).