ПРАВО НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ ТЕХНОЛОГИИ

ГРАЖДАНСКОПРАВНИ АСПЕКТИ

ЕЛЕКТРОННИ ДОКУМЕНТИ И ЕЛЕКТРОННИ ПОДПИСИ ЕЛЕКТРОННА ТЪРГОВИЯ ЗАЩИТА НА ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ В ИКТ ЗАЩИТА НА ПОТРЕБИТЕЛИТЕ В ИКТ

ГЕОРГИ Г. ДИМИТРОВ

Цитиране:

Димитров, Г., Право на информационните и комуникационните технологии. Гражданскоправни аспекти, Фондация „Право и Интернет“, София, 2014 г

Глава II. ЕЛЕКТРОННИ ДОКУМЕНТИ. ЕЛЕКТРОННИ ПОДПИСИ

2. ЕЛЕКТРОННИ ПОДПИСИ

2.1. Понятие и характеристики на саморъчния подпис

За установяване на авторството на писмените документи, законът е признал за правно-значим белег наличието на саморъчен подпис[120].

Наличието на подпис създава сигурност в правния мир за това кой е авторът на писменото изявление. Това е така, поради следните особености.

Първата функция на подписа е установяването на авторството върху изявлението. При саморъчния подпис по особеностите на движението на ръката, подобността на изображението и наличието на идентифицируеми знаци може посредством графологична експертиза да се установи със сравнително висока степен на увереност дали подписът е положен от твърдения автор.[121]

Втората функция на подписа е установяването на съгласието на автора с извършеното изявление. След като авторът е положил подписа си под писмения документ, той е съгласен с настъпването на правните последици от него. Иначе не би го подписал.[122]

Третата функция на подписа е постигането на интегритет на изявлението. Самият факт, че подписът се полага непосред-

---

[120] Вж. чл. 180 ГПК - частни документи, подписани от лицата, които са ги издали, съставляват доказателство, че изявленията, които се съдържат в тях, са направени от тези лица. За официалните документи наличието на подпис се подразбира – съгласно чл. 179 официален документ, издаден от длъжностно лице в кръга на службата му по установените форма и ред, съставлява доказателство за изявленията пред него и за извършените от него и пред него действия.

[121] Известно в чуждестранната правна наука като „authenticity“. Вж. Dumortier, J., ELDOC Legal Study on Legal and Administrative Practices Regarding the Validity and Mutual Recognition of Electronic Documents, With a View to Identifying the Existing Legal Barriers for Enterprises. Final Report, DG Enterprise & Industry, European Commission, 2006, p. 26.

[122] В чуждестранната литература - „consent“. *Пак там*.

ствено след изявлението, и че подписът и изявлението са неразривно обективирани върху един носител, създава сигурност, че волята на автора е тази, до където авторът се е подписал. [123] Всякакви зачерквания, изтривания, добавяния на текст преди или след подписа разколебават увереността относно волята на автора и съответно доказателствената стойност на документа.[124]

Четвъртата функция на подписа е осигуряването на правен стабилитет на документа, с оглед настъпването на правните последици и доказването на волята на автора във времето. Съставянето на документите е обусловено от необходимостта те да достигнат до съзнанието на други лица – адресати. Документите веднъж съставени циркулират в оборота и е необходимо дори и след време да може да се установи волята на автора, обективирана в тях и следователно настъпилите правни последици. Подписването на документите създава сигурност за оборота, че авторът няма да може след обективиране на подписването на изявлението да се „отметне“ и да оспорва последиците.[125]

Тези четири функции на саморъчния подпис в продължение на много години са обезпечавали сигурността на оборота относно стабилитета на писмените документи. Когато лицето е неграмотно, вместо подпис и като алтернатива може да се положи отпечатък от палец, а когато няма такъв – от друг пръст[126]. Приема се, че пръстовият отпечатък създава същата степен на сигурност както и подписа, но има редица неудобства - липсва характерният за под-

---

[123] В чуждестранната литература – „integrity“. *Пак там*.

[124] Съгласно чл. 178, ал. 2 ГПК съдът оценява доказателствената сила на документа, в който има зачерквания, изтривания, добавки между редовете и други външни недостатъци, с оглед на всички обстоятелства по делото.

[125] В чуждестранната литература - „non-repudiation“. Вж. Dumortier, J., *цит. съч.*

[126] Вж. чл. 189, ал. 1 ГПК - частен документ, издаден от неграмотен, трябва да носи вместо подпис отпечатък на десния му палец и да бъде приподписан от двама свидетели. Ако отпечатъкът на десния палец не може да бъде сложен, в документа трябва да се отбележи причината за това, както и с кой друг пръст е сложен отпечатъкът.

писите идентифициращ елемент – идентифициращи знаци и букви, форма на подписа и т.н., които лесно да позволяват на адресатите да идентифицират визуално авторите.

2.2. Понятие за електронен подпис

2.2.1. Общи бележки

С развитието на информационните технологии и особено на Интернет, възможността за размяна на електронни изявления мигновено, без териториални ограничения и на практика безплатно, доведе до пренасянето на голямата част от комуникацията между хората в електронната среда.[127] Доколкото с някои от тези изявления законът свързва настъпването на правни последици, се постави с острота въпросът как да се осигури доказването на авторството на електронните изявления и наред с това да се обезпечат останалите функции на саморъчния подпис – съгласие, интегритет и неотменимост. В търсене на решение на този въпрос се създаде концепцията за електронен подпис като аналог на саморъчния подпис в електронния свят. В България валидността на електронния подпис се санкционира с приемането на Закона за електронния документ и електронния подпис (ЗЕДЕП).[128]

За разлика от саморъчния подпис обаче, електронният подпис разкрива съвсем различна природа.[129] Законът урежда три вида електронни подписи, които ще бъдат разгледани последователно.

---

[127] Вж. Томова, Ж., „Електронният документ и електронният подпис“, Сп. „Български счетоводител“, бр. 1, януари 2005 г., Притурка

[128] Обн. ДВ. бр.34 от 6 април 2001 г., изм. ДВ. бр.112 от 29 декември 2001 г., изм. ДВ. бр.30 от 11 април 2006 г., изм. ДВ. бр.34 от 25 април 2006 г., изм. ДВ. бр.38 от 11 май 2007 г., изм. ДВ. бр.100 от 21 декември 2010 г.

[129] Вж. Димитров Г., Практическо приложение на електронните подписи. Обикновен електронен подпис, Сп. „Пазар и право“, Кн. 1, 2003 г.

2.2.2. Обикновен електронен подпис

Обикновеният електронен подпис е определен като родово понятие „електронен подпис“ в чл. 13, ал. 1 ЗЕДЕП. Съгласно този текст електронен подпис е всяка информация в електронна форма, добавена или логически свързана с електронното изявление, за установяване на неговото авторство. Определението е транспонирано от Директива 1999/93/ЕС.[130]

Обхватът на понятието електронен подпис е широко. Законодателят допуска квалифицирането като електронен подпис на „всяка информация в електронна форма“. Това включва както нарочно идентифицираща информация – изписване на име, инициали, псевдоним или друг идентифициращ израз или знак, който да бъде разпознат като електронен подпис, но така и служебна информация, която не може да бъде възприета чрез обичайно възпроизвеждане (служебна информация, придружаваща съобщението по електронна поща (S/MIME) в т.нар. „заглавка“, служебната информация, придружаваща SMS-съобщението съдържаща номера на викащия, идентификатора на интернет адреса, от където е извършено попълване и подаване на онлайн форма през стандартизирано уеб-базирано приложение и т.н., служебна информация от специализирано приложение, инсталирано на информационната система на потребителя към информационната система на адресата и др.).

Достатъчно е информацията да е добавена или логически свързана с електронното изявление. Законодателят подхожда при дефинирането на електронния подпис по технологично неутрален начин - технологията за добавянето или логическото свързване не е от значение. От съществено значение обаче, е тази информация да служи за идентифициране на автора. Идентифицирането може да е посредством сетивата, но може и чрез автоматизирано иден-

---

[130] Според чл. 2, т.1от Директивата „електронен подпис“ означава данни в електронна форма, които се добавят към или са логически свързани с други електронни данни, и които се използват като метод за установяване на авторството.

тифициране (например поради самия факт, че изявлението изхожда от специализирано приложение, което е под контрола на автора, адресатът се доверява на авторството или поради факта, че изхожда от точно определен IP адрес, адрес на електронна поща или мобилен номер).

Технологичната сигурност по отношение на това дали авторът е лицето, което действително е извършило изявлението също не е от значение за закона. Важното е страните да са се съгласили, че в отношенията помежду си ще приемат този подпис за достатъчно сигурен, така че да се изпълняват функциите на подписа – установяване на авторство, съгласие, интегритет и неотменяемост. В тази насока е и разпоредбата на чл. 13, ал. 4, предл. 2 ЗЕДЕП - страните могат да уговорят, че ще признават стойността на обикновения електронния подпис на саморъчен в отношенията помежду им.

С оглед на изложеното става ясно, че обикновеният електронен подпис черпи правната си сила на саморъчен от волята на страните. Веднъж съгласили се относно начина на идентифициране, страните не могат да оспорват, че изявлението не е подписано.

Съгласието може да е изрично, например нарочна клауза в договор, или да следва от конклудентни действия на страните – например обменят електронни изявления чрез определена технология (електронна поща, SMS, социална мрежа) и изпълняват задълженията си по възникналите правоотношения. То може да е предварително или последващо. Във всички случаи правоприлагащият орган трябва да изследва наличието на воля, за да се признае валидността на електронния подпис, придружаващ електронното изявление.[131]

---

[131] Необходимостта от признаване на правната стойност на обикновения електронен подпис произтича от транспонираното правило на чл. 5, ал. 2 от Директива 1999/93/ЕО - 2. Държавите членки гарантират, че правната сила и допустимост на електронния подпис като доказателство при съдебни производства не може да бъде оспорена единствено на основанието, че той е в електронна форма, или не се основава на квалифицирано удостоверение, издадено от акредитиран доставчик на удостоверителни услуги, или не е създаден от устройство за създаване на защитени подписи.

2.2.3. Усъвършенстван електронен подпис

Като друг вид електронен подпис законът регулира усъвършенстваният електронен подпис.[132] От семантичния анализ на дефиницията става ясно, че извън изискванията на обикновения електронен подпис, при усъвършенстваният трябва да е налице технологичен и логистичен инструментариум, който да обезпечава по-голяма сигурност за оборота, следователно по-голяма увереност у адресатите относно авторството на подписаните електронни изявления.[133]

Съгласно чл. 13, ал. 2 ЗЕДЕП усъвършенстваният електронен подпис е информация в електронна форма, добавена или логически свързана с електронното изявление, за установяване на неговото авторство[134], нооще трябва отговаря и на следните изисквания:

- да дава възможност за идентифициране на автора;
- да е свързан по уникален начин с автора;
- да е създаден със средства, които са под контрола единствено на автора;
- да е свързан с електронното изявление по начин, който осигурява установяването на всякакви последващи промени;[135]
- страните да са се съгласили, че ще признават правната сила на усъвършенстваният електронен подпис на саморъчен.[136]

На *първо място* е необходимо информацията да дава възможност за идентифициране на автора. Това е разбираемо. Първа-

---

[132] Димитров Г., Практическо приложение на електронните подписи. Усъвършенстван електронен подпис, Сп. „Пазар и право“, Кн. 2, 2003 г.

[133] Дефиницията на усъвършенстваният електронен подпис е транспонирана от чл. 2, т. 2 от Директива 1999/93/ЕС.

[134] Вж. арг. от чл. 13, ал. 1 ЗЕДЕП.

[135] Чл. 13, ал. 2 ЗЕДЕП.

[136] Чл. 13, ал. 4, предл. 2 ЗЕДЕП.

та и най-важна функция на електронния подпис е възможността за автентификация – установяване на авторството на електронното изявление. Адресатът трябва да изгради увереност, че изявлението изхожда от точно определен автор. Подобно на обикновения електронен подпис такава информация може да бъде възприемана от човешките сетива, но може да бъде и само машинно интерпретируема. Така например при ползване на електронно банкиране – типичен пример за използване на усъвършенствани електронни подписи, идентифицирането на служебната информация от токена, предоставен на клиента, е достатъчна сигурност за банката, че това е именно нейният клиент. Идентифицирането посредством потребителско име и парола, въвеждани на ръка от клиента, е друг способ за идентифициране на автора. Токенът или потребителското име и парола са предоставени на автора именно за да може той да се идентифицира пред адресата – банковата институция, за да извършва нареждания за плащания и други изявления спрямо нея. Фактът, че в системата на банковата институция е съхранена информация при сключването на договора с клиента на банката, че точи токен или това потребителско име и парола ще се ползват от него, създава увереност за банката, че точно клиентът, а не някой друг извършва изявлението. Разбира се, само това изискване не създава достатъчна технологична и логистична сигурност за оборота, необходимо е да са спазени и другите условия, за да се счете, че електронният подпис е усъвършенстван.

На *второ място* информацията трябва да е свързана по уникален начин с автора. Такъв начин предполага невъзможност на друго лице да използва информацията, за да се идентифицира. „Свързването“, означава обвързаност на информацията с определен автор. Механизмът и логистиката на подписване трябва да създава увереност у адресата, че използването на информацията не само изхожда от автора (т.е. да може да се идентифицира авторът, а и че подписът не може да изхожда от друго лице. В разглеждания по-горе пример банковата институция изгражда такава

увереност, като лично неин служител чрез съответни документи за самоличност идентифицира клиента на място и лично на него връчва срещу подпис токен с точно определен идентификатор или потребителското име и парола. Банката е уверена, че клиентът ще е автор на извършените изявления, защото точно нему е връчен токенът, съответно потребителското име и паролата.

На *трето място* усъвършенстваният електронен подпис трябва да е създаден със средства, които са под контрола на автора. Хипотезата на тази норма предполага изясняването на два момента – какво е средства за създаване на подписа и в какво се изразява осъществяването на контрол. По отношение на средствата за създаването на подписа – законодателят подхожда по технологично неутрален начин. Касае се за използване на такива технологични решения, които да осигурят функционалност за „подписване“. Такива биха могли да бъдат различни токени, мобилни телефони или компютърни системи, ведно с инсталираните приложения за изпращане на електронни изявления и др.под. От съществено значение е тези приложения да са под контрола единствено на автора. С други думи, единствено авторът трябва да има достъп (контрол) до тези средства, чрез които се осъществява подписването. Контролът може да е осигуряван чрез физическо държане на средствата за подписване или чрез обезпечаване на логически достъп до тях (през различни системи за отдалечен достъп – например чрез влизане с конкретен защитен профил в дадена система, до която и други лица имат физически достъп, но само авторът може да активира функционалността за подписване). В разглеждания по-горе пример за интернет банкиране – само авторът трябва да има достъп до токена за създаване на подписа.

На *четвърто място* елемент от фактическия състав, за да се квалифицира един електронен подпис за усъвършенстван е начинът на свързване на идентифициращата информация. Това трябва да става по начин, защитаващ съдържанието на електронното изявление от последващи промени, така че всяка промяна да мо-

же да се установи. Разглеждането на нормата през призмата на най-съвременните способи и методи за сигурна защита на съдържанието на предавани електронни пакети с информация може да доведе до неправилното ѝ тълкуване. Правилото не следва да се абсолютизира. При усъвършенстваните електронни подписи не е необходимо прилагането на такива методи за защита на съдържанието, които да разкриват максимално възможно ниво на сигурност. Достатъчно е ползването на методи чрез алгоритми на симетрична криптография (с един и същ ключ се криптира и декриптира съдържанието), използване на по-малко сигурни методи на асиметрична криптография (с различни ключове се извършва защитата и проверката), стандартизирани методи за защита, използвани при традиционните клиентски софтуерни приложения за размяна на електронни изявления и т.н. Идеята на законодателя е била да има някакво ниво на сигурност и на защита на съдържанието. Достатъчно е технологиите да обезпечават някакво ниво на сигурност и страните да го приемат за сигурно.[137] Така при изследваните примери за електронно банкиране ще се обезпечи достатъчна технологична сигурност за установяване на последващи промени в електронното изявление на следните технологии: криптиране на връзката посредством симетрични ключове, генерирани от токен устройството; използване на специализирани приложения за мобилно банкиране; при вече идентифициран с потребителско име и/или парола автор - изграждане на свързаност по различни протоколи (VPN, HTTPS, SFTP и др.); използване на асиметрични криптографски технологии, като сертификати за публичен ключ, генерирани от банката и съхранявани в информационната система на клиента, PGP и т.н.

На *пето място* следва да се отбележи, че така както обикновеният електронен подпис, усъвършенстваният черпи правната си стойност на саморъчен подпис от волята на страните. Те тряб-

---

[137] Димитров Г., Практическо приложение на електронните подписи. Усъвършенстван електронен подпис, *цит. съч.*

ва да са се съгласили, че ще приемат този начин на подписване за усъвършенстван електронен подпис. Доколкото всички посочени по-горе предпоставки са обективни и подлежат на доказване, то отново, както при обикновения подпис, волята на страните трябва да се изследва от правоприлагащия орган. Съгласието може да е предварително или последващо, манифестирано изрично или изразено с конклудентни действия.[138] Обичайно съгласието се обективира изрично и предварително в различни договорни клаузи, особено в банковото дело.

При наличието на всички предпоставки на чл. 13, ал. 2 и 4 ЗЕДЕП идентифициращата информация ще се счита за усъвършенстван електронен подпис с всички произтичащи от това правни последици.

2.2.4. Квалифициран електронен подпис.

2.2.4.1. Обща характеристика

Квалифициран електронен подпис е усъвършенстван електронен подпис, който в допълнение на изискванията, посочени по-горе, трябва да отговаря и на следните условия:

1. да е придружен от издадено от доставчик на удостоверителни услуги удостоверение за квалифициран електронен подпис, удостоверяващо връзката между автора и публичния ключ за проверка на подписа и
2. да е създаден посредством устройство за сигурно създаване на подписа.

Независимо, че може да не отговарят на нормативноустановените изисквания, усъвършенстваните електронни подписи на доставчиците на удостоверителни услуги и усъвършенстваните електронни подписи на Комисията за регулиране на съобщенията, с които тя подписва актовете, издавани въз основа на правомо-

[138] Вж. раздел 2.2.2, *по-горе*.

щията ѝ по закон, са приравнени на квалифицирани електронни подписи по силата на законова фикция.[139]

За разлика от обикновения и усъвършенствания електронен подпис, при квалифицирания електронен подпис като предпоставка липсва необходимостта о съгласуване на волята на страните за признаване на електронния подпис на правните последици на саморъчен. Квалифицираният подпис има значението на саморъчен подпис по отношение на всички по силата на закона.[140]

Макар законодателят да се опитва да създаде технологично неутрална уредба по отношение на електронните подписи, за квалифицирания електронен подпис този подход не може да бъде проведен докрай. Квалифицираният електронен подпис почива върху конкретна технология –инфраструктура на публичния ключ.[141] Преди да се изследват особените предпоставки за квалифицирания електронен подпис, следва да се анализира механизмът му на действие.

2.2.4.2. Механизъм на действие

Принципът на действието на квалифицирания електронен подпис се базира върху използването на двойка числа, наричани частен и публичен ключ. Тези числа не са еднакви, но са математически относими при прилагането на определен алгоритъм. Характерно е, че всяка двойка ключове е уникална. Това означава, че на един частен ключ отговаря само един публичен ключ. Друго характерно е, че от публичния ключ практически е невъзможно да се изведе частният ключ с най-съвременните информационни и технологични средства.

Създаването на ключовете по своята същност представлява генериране посредством съответни математически алгоритми на асиметрична криптография на двойката ключове и предоставяне-

---

[139] Вж. чл. 16, ал. 3, т. 1 ЗЕДЕП.

[140] Чл. 13, ал. 4, предл. 1 ЗЕДЕП.

[141] Инфраструктура на публичния ключ (Public Key Infrastrastructure – PKI).

то на частния ключ на автора. Този процес следва да става при строго спазване на законовите предписания, както към системите за създаване на тези ключове, така и към начините за физическото предоставяне на частния ключ на оправомощения автор.[142] В тежест на доставчика на удостоверителни услуги, предлагащ услугата по създаване на частен и публичен ключ, е вменено в задължение да не съхранява или копира данни за създаването на частните ключове.[143]

Това е така, защото частният ключ следва да бъде достояние единствено и само на автора. Никой друг няма право на достъп до тайната на частния ключ.[144] Само той се използва за „подписване" на електронното съобщение. Ако частният ключ стане достояние на друго лице, то същото ще може да подписва изявления от името на титуляря и да ангажира неограничено неговата правна сфера. Интересите на титуляря, респективно на обществото, сериозно биха били застрашени.

Публичният ключ може да бъде направен достояние на всички трети лица. С него се проверява дали полученото подписано съобщение не е променяно от момента на изпращането до момента да получаването и дали подписът е създаден с точно съответстващия му частен ключ.

Използването на един ключ за осъществяване на шифриране (криптиране) и различен ключ за дешифриране (декриптиране) е възможен благодарение на създадените алгоритмични методи на асиметрична криптография.[145]

---

[142] Калайджиев, А., Белазелков, Б., Димитров, Г., и авт. кол., *цит. съч.*, стр. 113.

[143] *Пак там*.

[144] Чл.14 ЗЕДЕП.

[145] Изискванията към алгоритмите за създаване на квалифициран електронен подпис са установени с Наредбата за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис (НИАСПКЕП). Допустимите алогоритми са: RSA (Rivest-Shamir-Adleman) с минимална дължина 1024, DSA (Digital Signature Algorithm) и ECDSA (Elliptic Curve Digital Signature Algorithm). Допуска се използване и на други алгоритми, за създаване на двойки ключове и за създаване на електронни подписи, които са с най-малко същото ниво на сигурност.

„Подписването“ на електронния документ с квалифициран електронен подпис се базира на извличането от даден електронен документ посредством определени алгоритми (хеш-алгоритми) на уникално математическо контролно число на този документ, наричано „хеш идентификатор“[146]. Характерно е, че извлеченото контролно число отговаря само на документа, от който е извлечено. С криптирането на контролното число с частния ключ се създава самият електронен подпис. С други думи усъвършенстваният електронен подпис е криптирано с частния ключ контролно число на електронния документ.

Както става ясно, електронният подпис се създава едва към момента на „подписването“ на определен електронен документ. За всеки електронен документ електронният подпис е различен, макар и създаден с един и същ частен ключ. Затова е не съвсем коректно да се казва, че някой „притежава електронен подпис“. Той притежава частен ключ за създаване на електронни подписи и публичен ключ за проверка на тези подписи.[147]

Практически след създаването на електронния подпис („подписването“), към електронното изявление се добавя преобразуваното с частния ключ контролно число (електронният подпис) и така добавеното и логически свързано съобщение в пакет се изпраща на адресата.[148]

В електронния документооборот от изключителна важност е да съществува сигурност, че изпращаните електронни изявле-

---

[146] Изискванията за хеш алгоритмите са посочени също в наредбата. Такива могат да бъдат SHA-1 (Secure Hash Algorithm), SHA-2 (224, 256, 384, 512 бита) и RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest) (256, 320 бита). Допуска се използването и на други хеш алгоритми, които са с най-малко същото ниво на сигурност. Дължината на идентификатора на електронното изявление следва да е не по-малка от 160 бита.

[147] Калайджиев, А., Белазелков, Б., Димитров, Г., и авт. кол., *цит. съч.*, стр. 85.

[148] Съществуват множество файлови формати, които допускат добавяне и логическо свързване на електронен подпис с електронно изявление. Такива често използвани файлови формати за структурирано и неструктурирано съдържание са: docx, doc, xlsx, xls, pdf, .odf, .xml, .ps7, .asf и др.

ния няма да могат да бъдат изменяни от недобросъвестни лица от момента на изпращането до момента на получаването им, и да може със сигурност да се установи кой е авторът на изпратеното съобщение. Тази увереност и сигурност се постига посредством проверка на подписа от адресата на подписаното електронно изявление.

Тоест проверката следва да даде отговор на два въпроса: 1) създаден ли е подписът със съответстващия му частен ключ и 2) променяно ли е подписаното съобщение от момента на изпращането на съобщението до момента на получаването му.

Проверката представлява огледален процес на този на подписването. Осъществява се чрез публичния ключ, който е направен достояние на адресатите. Първо адресатът декриптира електронния подпис и получава контролното число такова, каквото е било към момента на създаване на подписа. След това се извлича ново контролно число от електронното изявление и новополученото контролно число се сравнява с декриптираното. Ако проверката е успешна и те са идентични, то това означава, че изявлението не е променяно от момента на изпращането до момента на получаването. Ако съобщението е променено след подписването му, то проверката ще е неуспешна – добавянето или премахването дори на един бит информация от електронното изявление ще резултира в съвсем нов електронен документ, а следователно и новоизвлеченото контролно число ще се различава от декриптираното. Така лесно може да се установи нарушаване на интегритета на изявлението.

Подписването и проверката на електронния документ стават автоматично посредством специализиран софтуер (стандартизираните популярните софтуерни приложения – клиентски софтуери за електронна поща, браузъри и др. поддържат такава функционалност).

2.2.4.3. Устройство за сигурно създаване на подписа

За да се гарантира достатъчна сигурност, че при създаването на подписа няма да има възможност да се въздейства върху процеса на неговото създаване, трябва да се използват специални програмни или хардуерни системи и устройства. Те обезпечават високо ниво на сигурност и увереност, че процесът на създаване няма да бъде повлиян от случайни или непозволени външни въздействия. Тези устройства, се наричат устройства за сигурно създаване на подписа[149] и са уредени в чл. 17, ал. 1 ЗЕДЕП. Специална дефинитивна разпоредба определя, че устройство за сигурно създаване на подписа е „софтуер или хардуер, използван за въвеждане на данните за създаване на подписа“ (§1, т. 6 от ДР ЗЕДЕП).

Тези устройства трябва да гарантират, че: данните за създаване на електронния подпис могат да се използват само при създаването му и тяхната сигурност е надеждно защитена; данните за създаване на електронния подпис не могат да бъдат извлечени и подписът е защитен срещу подправяне; данните за създаване на електронния подпис могат да бъдат защитени от автора срещу използването им от други лица; съдържанието на изявлението е достъпно за автора и остава непроменено до създаването на електронния подпис.

Изискванията към сигурността на устройството за създаване на подписа в Европа са конкретизирани в различни референтни документи[150], като критериите и методите за проверка на ин-

---

[149] В чуждестранната литература – Secure Signature-Creation Devices (SSCD). Вж. чл. 3, ал. 2, т. 6 от Директива 1999/93/ЕС и Анекс III.

[150] Вж. CEN/ISSS CWA 14169 – „Secure Signature-creation devices ‘EAL 4+’“, CEN/ISSS CWA 14170 – „Security requirements for signature creation applications“, CEN/ISSS CWA 14172-5: „Secure signature creation devices“, CEN/ISSS CWA 14355 – „Guidelines for the implementation of Secure Signature-Creation Devices“, CEN/ISSS 14365-2 – „Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices“, CWA/ISSS 14892, който е трансформиран в Европейски стандарта с две части – „Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements“ и Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services“.

формационната сигурност (податливост на случайни или нарочни интервенции) са специфицирани в международния стандарт ISO 15408.[151]

Примери за такива устройства за сигурно създаване на подписа могат да бъдат смарт-карти, хардуерни крипто-модули, смарт-пен, мобилен телефон и др. Оценката дали едно устройство може да отговаря на изискванията за сигурно създаване на подпис се оценява от специализирани лаборатории, акредитирани да извършват такива проверки въз основа на съответни тестове. За извършените проверки се издава нарочен сертификат. [152]

Създаването на квалифицирания електронен подпис посредством устройство за сигурно създаване на подписа е една от необходимите предпоставки, за да се зачете валидността на електронния подпис като квалифициран. Липсата на такова устройство в процеса на създаването девалидира електронния подпис като квалифициран.[153]

Огледално на процеса на подписването, за който трябва да се използва устройство за сигурно създаване на подписа, лицата, които извършват проверка на усъвършенстван електронен подпис, трябва да прилагат устройство, което гарантира, че: данните за проверка на електронния подпис съответстват на данните, визуализирани пред лицето, извършващо проверката; подписът е надлежно проверен и резултатите от тази проверка са визуализирани пред лицето, извършващо проверката; съдържанието на подписаното изявление може да бъде надлежно установено; авторството и валидността на удостоверението за електронен подпис към момента на проверката са надлежно проверени; резултатите

---

[151] Още известен като „Общи изисквания“ или „Общи критерии“ - „Common Criteria“.

[152] Вж. чл. 6 НИАСПКЕП - Съответствието на устройството за сигурно създаване на подписа с изискванията на чл. 17, ал. 1 от Закона за електронния документ и електронния подпис се удостоверява с документ, издаден от акредитирана лаборатория за осъществяване на такава проверка.

[153] Арг. от чл. 16, ал. 1, т. 2 ЗЕДЕП.

от проверката и идентичността на автора са правилно възпроизведени; използването на псевдоним е ясно обозначено; всички промени, свързани със сигурността, могат да бъдат установени.[154], [155]

2.2.4.4. Удостоверение за електронен подпис

2.2.4.4.1. Понятие за удостоверение за електронен подпис

Както бе отбелязано, квалифицираният електронен подпис е средство за автентификация, базирано на използването на частния ключ на асиметрична криптосистема и проверка чрез публичния ключ на автентичността и интегритета на преобразуваното съобщение. Самото използване на частния ключ от автора за преобразуване на съобщението и съответната проверка от адресата чрез публичния ключ не гарантира обаче, че публичният ключ е притежание на лицето, което се представя за автор на съобщението.

Съществува риск недобросъвестно лице да генерира частен и публичен ключ и да подписва електронни документи с електронен подпис като се представя пред адресатите на съобщенията за друго лице. Проверката с публичния ключ ще установи, че съобщението не е променено и е подписано със съответстващия му частен ключ. Но по този начин не може да установи кой точно е титулярят на публичния ключ. Следователно само създаването и използването на частен и публичен ключ не може да създаде достатъчна сигурност в електронния документооборот по отношение авторството на електронните изявления. Липсва връзка между публичния ключ и неговия титуляр. Необходимо е прилагането на механизъм, чрез който да се установява по безсъмнен начин чие притежание е публичния ключ.

---

[154] Чл. 17 ал. 2 ЗЕДЕП.

[155] Известно в чуждестранната литература като „Secure Signature-Verification Device“. Относно техническите изисквания към устройствата вж. Анекс IV от Директива 1999/93/ЕО, а още и CEN/ISSS CWA 14171 – „General guidelines for electronic signature verification“.

Решението на проблема се крие в удостоверяването и гарантирането от трета доверена страна на връзката между публичния ключ и неговия титуляр - точно определено физическо или юридическо лице. Тази връзка се осъществява чрез издаването на електронно удостоверение за квалифициран електронен подпис. Третата доверена страна е дефинирана легално в нашия закон като „доставчик на удостоверителни услуги“ (ДУУ).

Удостоверението за електронен подпис е специален електронен документ, съдържащ името на титуляря и неговия публичен ключ и други предписани от закона реквизити.[156] Това удостоверение се подписва с квалифицирания електронен подпис на доставчика. Удостоверението се изпраща на адресата в пакет заедно с електронното изявление и електронния подпис, свързан с изявлението. Доколкото се предполага, че всички трети лица ще могат да проверят верността на публично достъпните публични ключове на доставчиците на удостоверителни услуги, то се създава увереност и сигурност у тях, че публичният ключ, който е вписан в издаденото удостоверение, е действително притежание на автора на подписа. По този начин всички трети лица – адресати на електронни съобщения, подписани с квалифициран електронен подпис на автора, ще могат да установят дали изпратеното съобщение изхожда точно от него, тоест дали съобщението е автентично. Следователно, за да се издаде удостоверение е необходимо доставчикът на удостоверителни услуги да се убеди и провери самоличността на автора и фактите, че частният ключ се държи от него и че представеният публичен ключ, съответства именно на държания от автора частен ключ. Целият този процес на проверка протича съобразно предписанията на закона и правилата за сигурност на доставчика на удостоверителни услуги. Крайната фаза, целеният акт е издаването на удостоверение. Издаването на удостоверението се осъществява чрез вписването му в публично

[156] Вж. чл. 24 ЗЕДЕП.

достъпен електронен регистър на удостоверенията, поддържан от доставчика.[157]

Наличието на валидно придружаващо удостоверение е предпоставка квалифицираният електронен подпис да се приеме за валиден.

Липсата на някои от задължителните реквизити опорочава удостоверението и то загубва качеството си на удостоверение за квалифициран подпис. Респективно, ако такова невалидно удостоверение придружава електронния подпис, то същият се девалидира, а подписаният с него документ ще се счита неподписан с квалифициран електронен подпис. Такива ще са последиците и ако удостоверението е с изтекъл срок или е било прекратено действието му предсрочно.

Следва изрично да се отбележи, че смисълът на удостоверението е да се удостоверява притежанието на публичния ключ за проверка на авторството на подписаните с квалифициран електронен подпис електронни изявления. Смисълът на удостоверението не е да се удостоверява самоличността на авторите. Поради тази причина е неправилно третите лица да се доверяват на вписаните в удостоверението атрибути като ЕГН, лична карта и други, които доставчикът съгласно закона няма право да удостоверява. За тях удостоверението няма официална удостоверителна сила, а има характер на частно удостоверяване. За установяване на самоличността на лицата в електронния свят съществува друга концепция, която почива върху различни удостоверявания.[158]

Издадените и прекратените удостоверения се публикуват в нарочни списъци в специален регистър при доставчика и тяхната валидност може да се провери по всяко време, включително и

---

[157] Става дума за X.500 регистър. вж. раздел 2.2.4.4.4, *по-долу*.

[158] Вж. Пилотен проект за електронна идентичност, http://eid.egov.bg.

автоматизирано от специализирани софтуерни приложения, поддържащи функционалност за подписване и проверка на подписани съобщения.[159]

2.2.4.4.2. Издаване за удостоверение за електронен подпис

Издаването на удостоверение за електронен подпис става по писмено искане на автора.[160] Доколкото писмената форма се счита спазена, ако е съставен електронен документ[161], то договорът може да се сключи и в електронна форма.

Удостоверение може да бъде издадено, ако удостоверяваните с него факти бъдат истинни. Така всички трети лица ще им се доверяват и ще направляват съответно поведението си. Липсата на истинност би довела до заблуда у третите лица и това би ги мотивирало да приемат решения и извършват действия в заблуда и грешка, което би рефлектирало в нежелани правни последици и вреди. Невярното удостоверяване би повлякло отговорността на ДУУ.[162] В тази връзка, е от изключително значение доставчикът да положи дължимата грижа, за да издаде удостоверение само, ако са налице истинни обстоятелства – предпоставка за издаването.

Доставчикът ще издаде удостоверение само тогава, ако искането изхожда от автора или от надлежно овластено от него лице – само надлежно овластеният от титуляря автор или представител на последния може да заяви издаването на удостоверението.[163] Никой не може да поиска издаване от чуждо име без представителна власт – доставчикът следи служебно и проверява този факт. Представителната власт може да произтича от сделка (упълномо-

---

[159] Проверки могат да се осъществяват чрез уеб-базирано приложение по стандартизиран протокол (напр. HTTP), както и посредством други протоколи – LDAP (Lightweight Directory Access Protocol) и OCSP протокол за автоматизирана проверка на удостоверенията (Online Certificate Status Protocol).

[160] Чл. 25, ал. 1 ЗЕДЕП.

[161] Чл. 3, а. 2 ЗЕДЕП.

[162] Чл. 29 ЗЕДЕП.

[163] Чл. 25, ал. 1, т. 1 ЗЕДЕП.

щаване, договор за поръчка) или от закона (представителство на юридическо лице, представителство на деца от техните родители, представителство на поставени под пълно запрещение от техните настойници, представителство на държавни юридически лица от органите, представляващи ги по закон и т.н.).

На следващо място информацията относно автора, представена за включване в удостоверението, трябва да е вярна и пълна.[164] Такава информация ще бъде името или псевдонимът на автора на електронния подпис и особени атрибути, свързани с автора, ако удостоверението се издава за конкретна цел, както и ако доставчикът поддържа политика за издаване на удостоверения с вписване на такива атрибути (например адрес, упражняване на свободна професия, принадлежност към определена общност и т.н.).

Доколкото с удостоверението се атестира принадлежността на публичния ключ за проверка на квалифицирания електронен подпис на точно определен автор, то той трябва да притежава частния ключ. Доставчикът следва да провери този факт.[165] Частният ключ не само трябва да се държи от автора, но и да е технически годен да бъде използван за създаване на квалифициран електронен подпис. Чрез него трябва да може да се подписват електронни изявления посредством установените алгоритми на асиметрична криптосистема. Техническите и алгоритмични изисквания към него са нормативно установени.[166] Освен това, частният ключ трябва да съответства алгоритмично на подлежащия на удостоверяване публичен ключ, така че чрез публичния ключ да може да се удостовери, че определен квалифициран електронен подпис е създаден с частния ключ. В противен случай успешна алгоритмична проверка на електронния подпис не би могла да се извърши от адресатите на подписаните електронни изявления.

---

[164] Чл. 25, ал. 1, т. 2 ЗЕДЕП.

[165] Чл. 25, ал. 1, т. 3 ЗЕДЕП.

[166] Вж. глава II и Приложението към НИАСПКЕП и раздели 2.2.4.2 и 2.2.4.3, *по-горе*.

Когато авторът действа в точно определено качество по отношение на конкретен титуляр (напр. юридическото лице плаща за удостоверителната услуга за издаване на удостоверение на изпълнителния директор, който ще подписва документи само в това му качество) и се иска вписване в удостоверението на титуляря, от името на когото ще се извършват изявленията, искането се удовлетворява, ако са спазени изискванията по отношение на истинността на данните на автора и на притежавания от него частен ключ, но още трябва да е налице истинност по отношение на данните на титуляря и представителната власт на лицето, което от негово име иска издаване на удостоверението.[167]

Удостоверението се издава чрез вписването му в регистъра на удостоверенията. Авторът и титулярят в тридневен срок от публикуването на удостоверението могат да възразят, ако то съдържа грешки или непълноти. Въвеждане на промени в съществуващо удостоверение е технологично невъзможно – то е подписан електронен документ. Грешки се отстраняват незабавно от доставчика чрез издаване на ново удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на неверни данни от страна на автора, респ. титуляря. При липса на възражение в указания срок, се смята, че съдържанието на удостоверението е прието.

Удостоверението е достъпно и може по всяко време да се изтегли от регистъра. В процеса на издаването обичайно доставчикът го записва върху смарт-картата или друго устройство за сигурно създаване на подписа, което ще се използва от автора за нуждите на подписването. На практика с полагането на квалифициран електронен подпис удостоверението се прикача и логически свързва с подписания електронен документ. Поради тази връзка законодателят реферира към факта, че електронният под-

[167] Чл. 25, ал. 2.

пис се „придружава“ с издадено от ДУУ удостоверение за квалифициран електронен подпис.[168]

2.2.4.4.3. Спиране, възобновяване и прекратяване на удостоверение за електронен подпис

Наличието на валидно удостоверение, съпътстващо квлифицираният електронен подпис, осигурява увереност у адресатите относно принадлежността на публичния ключ и съответно авторството на създадения подпис. Доколкото сигурността на електронния оборот и интересите на адресатите са поставени в зависимост от наличието на едно удостоверение, то следва да съществува възможност при промяна в обстоятелства, които могат да застрашат верността на удостоверените факти и изграждането на увереност у адресатите, действието на удостоверението да бъде временно или окончателно преустановено.[169]

Така например при откradване на смарт-картата, на която е записан частният ключ на автора, и узнаването на ПИН-а за достъп, се създава опасност едно лице да подписва от името на друго лице електронни изявления. Все така оттеглянето и ограничаването на представителната власт на автора спрямо титуляря създава опасност неовластеният вече автор да продължи да прави изявления от името на титуляря. При наличие на такива обстоятелства в дадените примери, удостоверените в издаденото удостоверение факти съответно за принадлежността на публичния ключ, за правото на един автор да прави валидни изявления от името на титуляря, за правото на титуляря със свои електронни изявления да ангажира патримониума си, са неверни и повече не следва да се ползват с доверието на адресатите.

---

[168] Вж. чл. 16, ал. 1, т. 1 ЗЕДЕП - квалифициран електронен подпис е усъвършенстван електронен подпис, който е придружен от издадено от доставчик на удостоверителни услуги удостоверение за квалифициран електронен подпис, отговарящо на изискванията на чл. 24 и удостоверяващо връзката между автора и публичния ключ за проверка на подписа.

[169] Вж. Калайджиев, А., Белазелков, Б., Димитров, Г. и др, *цит.съч.*, стр. 221-238.

Законодателят е установил правен механизъм за промяна на статуса на едно удостоверение, която промяна да създаде съответен щит за интересите на третите лица и на титуляря чрез довеждането до знанието на третите лица на промяната на статуса на удостоверението и „лишаването“ му от удостоверителна сила. Този механизъм следва да се привежда в изпълнение лесно и бързо.[170]

Преустановяване на удостоверителната сила на едно удостоверение може да е временна или окончателна. Временното преустановяване се нарича спиране, а окончателното – прекратяване. Предпоставките за спиране и прекратяване са уредени в чл. 26 и чл. 27 ЗЕДЕП.

От изложеното става ясно, че спирането на действието на удостоверението представлява временно суспендиране на удостоверителната сила на издаденото удостоверение и се изразява във включване на удостоверението в списъка на прекратените удостоверения в регистъра на доставчика. Спирането на действието на удостоверението води до автоматично лишаване от правна стойност на всички положени усъвършенствани електронни подписи от момента на спирането.

При установяване липсата на обстоятелства, застрашаващи интересите на титуляря и третите лица, или при отпадането на съмненията за наличието им, статусът на удостоверението като „действащо“ следва да се възобнови и по този начин да се направи възможна проверката на всички подписи, положени от момента на спирането до момента на възобновяването, както и след това.

Политика на спиране може въобще да не се поддържа от доставчика на удостоверителни услуги. В такъв случай липсата на възможност за спиране следва да е облечена в съответна дого-

[170] *Пак там*, стр. 221.

ворна клауза в сключения с него договор за удостоверителни услуги.[171] В противен случай ще се прилагат законовите правила за спиране.

Ако политика за спиране е поддържана от ДУУ, то спиране могат да поискат няколко групи лица.

На *първо място* спиране може да се осъществи по инициатива на доставчика. Той може да спре действието на удостоверението при основателно съмнение, че то следва да бъде прекратено. Такива обстоятелства са всички визирани в чл. 27, включително компрометиране на тайната на частния ключ.

На *второ място* легитимирани да поискат спирането съгласно чл. 26, ал. 2 са титулярят, съответно авторът, лица, за които според обстоятелствата е видно, че могат да знаят за компрометиране на частния ключ, както и Комисията за регулиране на съобщенията. За титуляря и автора не може да има съмнение защо могат да искат спиране – те се ползват от удостоверителната услуга, те могат да поискат да не се ползват от нея, независимо какви са им мотивите. Спирането следва да се извършва бързо, за да не се допусне засягане правата на титуляря, поради което ДУУ трябва да спре действието веднага, без необходимост да се увери в самоличността на автора чрез представяне на сериозни доказателства. Не би могло да бъде и другояче – авторът вече се е легитимирал пред ДУУ при сключването на договора, освен това електронният подпис е на автора. Когато в удостоверението е вписан титуляр, авторът вече е и представил доказателства за представителната си власт спрямо титуляря. Не така стои въпросът със спиране на удостоверението по искане на титуляря, когато такъв е вписан в удостоверението. Макар неговата правна сфера да се засяга от извършените от автора действия, той следва да докаже и да се легитимира със съответни документи пред доставчика, за да може удостоверението да бъде спряно. Волята на законодателя е разби-

[171] Чл. 23 ЗЕДЕП.

раема. Чрез изявлението на титуляря ще се интервенира във възможността друго лице - авторът да използва електронния подпис. Следователно ДУУ трябва да е уверен, че именно и само титулярят е лицето, което като правоимащо е поискало това.

На *трето място* могат да искат спиране друг кръг лица, които според обстоятелствата могат да знаят за компрометиране на частния ключ. Законодателят неизчерпателно изброява такъв кръг лица - представители, съдружници, служители, членове на семейството и др. Лицата следва да се легитимират и ДУУ следва да провери самоличността им и да се информира относно обстоятелствата, които поставят тези лица в знание относно компрометирането на частния ключ.

На *четвърто място* спиране действието на удостоверението може да поиска и КРС. В качеството на регулаторен орган тя може да установи обстоятелства, които могат да навеждат на основателно съмнение, че действието на едно или повече удостоверения следва да бъде прекратено. Тогава тя ще извести доставчика, за да може последният да спре действието на удостоверенията.

Правото на КРС да поиска спиране следва да се отграничава от правото на председателя на КРС при непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона да задължи съответния доставчик на удостоверителни услуги да спре действието на удостоверението. В този случай, за разлика от хипотезите по ал. 1 и 2, ДУУ не може да преценява дали да спре или не удостоверението, тъй като преценката за наличието на потенциално увреждащи обстоятелства е направена от държавния орган, регулиращ дейността на доставчиците - КРС. Няма значение и дали има уговорка с титуляря, изключваща политиката на спиране. Доставчикът е длъжен да спре удостоверението.

Няма изискване в ЗЕДЕП относно начина на уведомяване на доставчика. То може да се осъществи по всякакъв начин. Предвид необходимостта от бързина при спирането, уведомяване е до-

пустимо дори по телефон, електронна поща, факс, лично явяване пред доставчика или по друг подходящ начин.[172] Начинът на уведомяване зависи от политиката на доставчика.

Доколкото различни групи лица могат да упражнят право, с което да се спре възможността авторът валидно да подписва с квалифициран електронен подпис електронни документи, то във всички случаи недобросъвестното упражняване на това право от някое от овластените по чл. 1 – 3 лица ще доведе до ангажиране на гражданската им отговорност за причинените от неоснователното спиране вреди.[173] Освен изложеното, то не може да е неограничено във времето. Законодателят определя че срокът за спиране е според обстоятелствата, но не повече от 48 часа.[174]

Ако срокът за спиране е изтекъл и удостоверението не е прекратено, то действието му се възобновява автоматично.[175]

Предвид факта, че спирането създава правна невъзможност от използване на удостоверението и доказване автентичността на електронно подписани документи, авторът и титулярят следва да бъдат незабавно уведомени от ДУУ, за да може да направят преценка дали обстоятелствата, касаещи компрометирането на частния ключ наистина са налице и дали действието на удостоверението следва да бъде окончателно прекратено или при липса на опасност - възобновено. Нормата на чл. 26, ал. 4 задължава ДУУ да извърши това. Доколкото уведомяването следва да стане незабавно, то това може да стане по телефона, чрез електронна поща, SMS или по какъвто и да е друг начин, налагащ бързо достигане на факта на спирането до автора и титуляря.

---

[172] Вж. Калайджиев, А., Белазелков, Б., Димитров, Г. и др, *цит.съч.*, стр. 224.

[173] *Пак там*.

[174] Чл. 26, ал. 1 – 3 ЗЕДЕП.

[175] Чл. 26, ал. 6, т. 1 ЗЕДЕП.

При спиране на действието на удостоверението, същото се вписва в списъка на прекратените удостоверения[176], публикуван в публичния регистър на удостоверенията на доставчика като временно прекратено.[177]

Спирането на действието на удостоверението има важни правни последици. То изключва възможността да бъдат проверявани подписите през времето от спирането до възобновяването, т.е. адресатите, получили подписани електронни изявления в този период от време, не следва да им се доверяват. От тяхна гледна точка неуспешната проверка на действието на удостоверението ще означава липса на валиден подпис. Адресатите ще съобразят вземането на решения си с този факт.

Спирането на удостоверението следва да се различава от прекратяването. Разликата се открива във времето, през което удостоверението е лишено от действие.

При спирането този период от време се определя от доставчика или от КРС, в зависимост от основанието за спирането и както стана ясно не може да бъде по-голям от 48 часа. След изтичане на този срок, или ако това е поискано от титуляря или автора преди изтичането му, удостоверителната сила на удостоверението се възобновява. Удостоверението се заличава от списъка с прекратени удостоверения.

При прекратяването на действието на удостоверението отпада занапред неговата удостоверителна сила, т.е. електронните документи, подписани след прекратяването на удостоверението, се считат неподписани. При прекратяването, действието на удостоверението се преустановява окончателно и необратимо. Изваж-

---

[176] Certificate Revocation List (CRL).

[177] Според стандарта X.509 v.2, в списъка на прекратените удостоверения спряното удостоверение се отбелязва в съответното поле за „основание за прекратяване“ с код „спряно удостоверение“ („suspended“). Само вписване обаче, не е достатъчно. Трябва списъкът да е подписан от доставчика и да е публикуван в регистъра. Едва от този момент спирането има ефект спрямо третите лица. За повече подробноси вж. раздел 2.2.4.4.4, *по-долу*.

дането на удостоверението от списъка на прекратените удостоверения е недопустимо.

Доколкото спирането само временно парализира удостоверителната сила на удостоверението, ако действието на удостоверението бъде възобновено, ефектът на спирането отпада. Ако спирането бъде последвано от прекратяване, ефектът на прекратяването настъпва от момента на спирането, т.е. спирането антиципира ефекта на последващото го прекратяване – всички документи, подписани по време на спирането, се считат неподписани.

Валидирането на подписите, положени от момента на спирането до момента на възобновяването, настъпва с обратно действие. Това означава, че документите, подписани по време на спряно удостоверение ще се считат валидно подписани, ако действието на удостоверението се възобнови.[178]

Възобновяване на действието на удостоверението се извършва в една група случаи автоматично, след изтичане на срока, за който то е спряно, и независимо от основанието и инициативата за спиране.[179] Тази предпоставка се реализира, ако междувременно действието на удостоверението не е прекратено. Това означава, че доставчикът трябва да поддържа такава функционалност на системите си или да е създал такава организация на работните си процеси, която да обезпечава незабавно възобновяване след изтичане на срока.

В други случаи възобновяването се извършва преди изтичането на срока за спиране - при отпадане основанието за спиране или при искане на титуляря или автора. Разбира се, във втория случай доставчикът следва да се увери, че титулярят и авторът

---

[178] Обратното в Калайджиев, А., Белазелков, Б., Димитров, Г. и др., *цит. съч.*, стр. 229. Различната правна трактовка идва от факта, че с измененията на ЗЕДЕП от 2010 г. се въведе изричната разпоредба на чл. 26, ал. 7 - възобновяването на действието на удостоверението заличава правните последици на спирането.

[179] Чл. 26, ал. 6, т. 1 ЗЕДЕП.

са узнали причината за спирането и възобновяването е поискано именно вследствие на узнаването.

Възобновяване може да се поиска от титуляря и от автора.[180]

Прекратяването на действието на удостоверението преустановява окончателно удостоверителната му сила. Прекратяването също се реализира чрез вписване на удостоверението в списъка на прекратените удостоверения, с осигуряване на неограничена във времето възможност за проверка на удостоверенията в този списък. Списъкът на прекратените удостоверения се публикува в регистъра на доставчика.[181]

С оглед сериозните правни последици на окончателното прекратяване на действието на удостоверението се налага установяването на по-строги изисквания по отношение възможността за прекратяването, отколкото при спирането.

Предпоставките, при които се прекратява действието на удостоверението, условно могат да се обособят в три групи – прекратяване поради обстоятелства, несвързани с титуляря и с автора, прекратяване по волята на титуляря или на автора и прекратяване поради обстоятелства, свързани с титуляря и с автора. Трите групи предпоставки са предмет на хипотезите съответно на трите алинеи на чл. 27 ЗЕДЕП.

Първата група основания са факти, настъпването на които прекратява автоматично действието на удостоверението – изтичането на срока на удостоверението, смърт или поставяне под запрещение на физическото лице – доставчик на удостоверителни услуги и прекратяването на правосубектността на юридическото лице на доставчика на удостоверителни услуги, когато доставчи-

---

[180] Обратното в Калайджиев, А., Белазелков, Б., Димитров, Г. и др., *цит. съч.*, стр. 230. Отново причината се корени в измененията на ЗЕДЕП от 2010 г.

[181] Вж. чл. 37, т. 3 от Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги (НДДУУРНПИПУУ).

към преди прекратяването на дейността си не я е прехвърлил на друг доставчик.[182]

Наличието на тези обстоятелства не налага вписването на удостоверението в списъка на прекратени удостоверения.[183] Настъпването на тези факти, обосноваващи автоматично прекратяване в повечето случаи не е, а и не може да бъде обусловено от волята на доставчика, макар че доставчикът е длъжен да направи това при установяването на факта – основание за прекратяване.

Ако доставчикът е прехвърлил дейността си на друг доставчик, действието на издадените удостоверения се запазва.

Втората група основания са свързани с прекратяване на действието на удостоверението по волята на автора и на титуляря. Използването на електронната форма за извършване на изявления е доброволно.[184] Титулярят може да преустанови използването на електронния подпис на автора по своя воля, изразена лично. Това право има и овластеният автор – частният ключ е негов. Причините са без значение за правото. Разбира се, доставчикът трябва по безсъмнен начин да се увери, че волята за това се изявява точно от титуляря или от автора. За установяване на самоличността, респ. идентичността на титуляря или на автора доставчикът може да използва всички допустими от закона средства.[185] При прекратяване на това основание, удостоверението се вписва в списъка на прекратените удостоверения.

---

[182] Чл. 27, ал. 1 ЗЕДЕП.

[183] При липса на прехвърляне на дейността на друг доставчик, регистърът на доставчика се прехвърля и се поддържа от КРС до изтичане срока на действащите удостоверения и 10 години след това. Инфраструктурата на публичния ключ и правната стойност на удостоверенията за универсален подпис налагат да се осигури във времето възможността за проверка на изтеклите удостоверения и на тези с прекратено действие, независимо от основанието за прекратяването. Вж. чл. 44 НДДУУРНПИПУУ.

[184] Вж. раздел 1.5.3 от тази глава, *по-горе*, и чл. 5 ЗЕДЕП.

[185] Вж. Калайджиев, А., Белазелков, Б., Димитров, Г. и др., *цит. съч.*, стр. 236.

Третата група основания за прекратяване са свързани с обстоятелства извън волята на титуляря и на автора, но свързани с тяхната правосубектност, дееспособност или упражнявани от тях права. Така наложително е действието на удостоверението да бъде прекратено при смърт или поставяне под запрещение на титуляря или на автора. Авторът и титулярят трябва да са дееспособни лица, за да могат да използват електронни подписи, за да изявяват правновалидна воля в електронна форма. Когато титулярят е юридическо лице, само тогава може да се ангажира правната му сфера, с оглед наличието на правосубектност. Следователно, всяка промяна в правосубектността, респ. дееспособността на титуляря или на автора, следва да влече прекратяване действието на удостоверението.

Когато в удостоверението е вписан титуляр, различен от автора, прекратяване на представителната власт на автора е друго основание за прекратяване. Такива удостоверения се издават обичайно на автори, които са служители или представляващи титуляря или лица, които са в договорна връзка на представителство с титуляря – счетоводители, адвокати, одитори и т.н. Те могат да извършват електронни изявления и да ги подписват, защото титулярят им е възложил това и ги е овластил. Прекратяването на представителната власт повлича необходимостта от прекратяване на удостоверението – авторът повече не може да упражнява права от чуждо име. При заявяване на това обстоятелство от титуляря, доставчикът е длъжен да прекрати удостоверението.

Друго основание за незабавно прекратяване действието на удостоверението е установяването, че удостоверението е издадено въз основа на неверни данни. Без значение е дали са предоставени съзнателно от автора при издаване на удостоверението или са вписани поради грешка.

Инициативата за прекратяването при третата група основания може да дойде от титуляря, автора, доставчика, трето лице или въз основа на данни, които доставчикът сам е узнал. Титулярят или авторът не могат да се противопоставят на прекратяването. Доставчикът следва да прекрати удостоверението, дори против волята на титуляря, респ. автора.

2.2.4.4.4. Регистър на удостоверенията

Функцията на доставчика на удостоверителни услуги е чрез предоставянето на удостоверителните услуги да създава в електронния документооборот увереност у адресатите на подписани електронни изявления относно валидността на квалифицирания електронен подпис и самоличността на неговия автор. Валидността на подписа е предпоставена от придружаването на подписа от валидно и действащо удостоверение за публичния ключ на автора. Докато срокът на удостоверението лесно може да се провери от използваните от адресата стандартизирани софтуерни решения за получаване на електронни изявления (приложения за електронна поща, приложение за текстообработка и др.), то другите обстоятелства, свързани с валидността на удостоверението – спиране и прекратяване, могат да се установят само при преглед на водения от доставчика специален публичен регистър. В него се вписват издадените удостоверения и списъкът на спрените или прекратени предсрочно удостоверения.

Успешната проверка на валидността на публикувано в регистъра удостоверение създава необходимата у адресата увереност да счита направените от автора електронни изявления за валидни и го мотивира да предприеме съответни правнорелевантни действия или да се въздържи от такива.

Воденето на регистър на издадените удостоверения има изключително значение за правната сигурност в оборота. При наличие на правен спор между титуляря и адресата на подписани из-

явления по отношение на валидността на подписа, доставчикът ще играе изключително важна роля за доказване на онези обстоятелства, които са свързани с оспорваната валидност, а именно – действието на удостоверението към определен момент във времето. От пазените логове и журнални записи ще може по безсъмнен начин да се установи статусът на удостоверението, а от там и валидността на подписа. Доставчикът на удостоверителни услуги е длъжен да осигури съответна техническа и технологична обезпеченост в тази насока.[186]

В регистъра се публикуват две групи обстоятелства.

На първо място, разбира се, доставчикът е длъжен да публикува удостоверенията за електронен подпис, които използва в дейността си като доставчик, издадените удостоверения и списъка на прекратените удостоверения. Какви са тези подлежащи на вписване обекти?

Доставчикът може да има различни двойки ключове, използвани за различни нужди. Инфраструктурата на публичния ключ почива върху не сложна йерархична конструкция. За да могат информационните системи на адресатите да осъществяват проверка на електронните подписи, те трябва да разпознават доставчика на удостоверителни услуги като доверен доставчик, а издадените от него удостоверения за електронен подпис като доверени. Това се постига чрез поддържането на списъци с доверени доставчици.[187] В базите данни на информационните системи обичайно се инсталира базовото удостоверение за публичния ключ на доставчика (Root Certificate) и неговите операционни удостоверения (Operational Certificates, Time-Stamp Certificates и др.). Частният ключ на базовата двойка ключове (Root Keys) обикновено се използва за подписване на самото базово удостоверение и на удостоверенията за операционните ключове на доставчика

[186] Чл. 32, ал. 2, т. 8 НДДУУРНПИПУУ.

[187] Trusted Certification Authorities.

(Operational Certification Authority Keys, Time-Stamp Certification Authority Keys и др.). Базовото удостоверение се използва само за да придружава подписаните с базовия електронен подпис базово удостоверение и операционни удостоверения. Удостоверението за базовата двойка е самоиздадено и самоподписано с базовия частен ключ.

С операционните частни ключове на доставчика се подписват удостоверенията на крайните потребители (авторите) за квалифициран електронен подпис и за време. Операционните електронните подписи върху удостоверенията на потребителите са придружени от операционните удостоверения. Съгласно закона, доставчикът вписва именно самоиздадените базови и операционни удостоверения, които ще ползва в дейността си на доставчик на удостоверителни услуги.

Освен тях, доставчикът вписва в регистъра и всички издадени удостоверения за квалифициран електронен подпис и удостоверенията за време.[188] Те се вписват в специална директория на регистъра с точно определени описатели, съгласно стандарта X.500. Веднъж извършени вписвания на удостоверения, повече промени по тези вписвания не могат да се извършват. Това е така, защото регистърът се подписва от доставчика на удостоверителни услуги след всяко вписване.

Доставчикът публикува и списък на прекратените удостоверения.[189] В списъка се публикуват всички спрени и прекратени удостоверения преди изтичането на срока им. Списъкът съдържа стандартни полета като версия на профила, име и националност на доставчика, дата на издаване, време на следващо обновяване, алгоритъм на подписа на списъка, номер на списъка, ключов

[188] Чл. 40 ЗЕДЕП.

[189] Вж. раздел 2.2.4.4.3 от тази глава, *по-горе*. Списъкът се води в специален формат, а файлът се обозначава с разширение „.crl“.

идентификатор на доставчика, публикуваните удостоверения, всяко със серийния му номер, дата и време на прекратяване и основание (код) за прекратяването[190]. Списъкът също се подписва електронно от доставчика.

На второ място, доставчикът на удостоверителни услуги публикува в регистъра и следната информация, от която потенциалните потребители на услугите му да могат да се ориентират за условията, при които тези услуги се предоставят и за дейността на доставчика: условията и реда за издаване на удостоверение, включително за правилата за установяване идентичността на титуляря на квалифицирания електронен подпис; процедурите за сигурност на доставчика на удостоверителни услуги; начина на използване на квалифицирания електронен подпис; условията и реда за използване на квалифицирания електронен подпис, включително изискванията за съхраняване на частния ключ; условията за достъп до удостоверението и начина на проверка на квалифицирания електронен подпис; цената за получаване и използване на удостоверение, както и цените на останалите услуги, предоставяни от доставчика на удостоверителни услуги; отговорността на доставчика на удостоверителни услуги и на титуляря на квалифицирания електронен подпис; условията и реда, по които авторът, съответно титулярят прави искане за прекратяване действието на квалифицирания електронен подпис. Публикуването на тази информация е само съпътстващо основните обекти, подлежащи на публикуване. То има само оповестително действие, с оглед информиране на потребителите за различните обстоятелства.[191]

---

[190] Когато удостоверенията са прекратени, кодовете, които се отбелязват в съответното поле на списъка могат да бъдат: компрометиран частен ключ; компрометиран частен ключ на доставчика; промяна в представителната власт на автора спрямо титуляря; заместване на удостоверението с друго.

[191] Вж. например регистрите на „Информационно обслужване“ АД (http://www.is-bg.net/bg/page/38), „Борика-Банксервиз“ АД (http://www.bobs.bg/bg/services), „Инфонотари“ АД (http://www.infonotary.com/site/?), „СЕП България“ АД (http://sep.bg/).

Изброените обстоятелства и информация обичайно се съдържат в Наръчника на потребителя на доставчика на удостоверителни услуги.[192] Ако доставчикът публикува своя Наръчник, то следва да се счита, че е изпълнил и условията по чл. 28, ал. 3.[193]

За да изпълни функцията си, регистърът трябва да е достъпен непрекъснато 24 часа в денонощието, 7 дни в седмицата. Прекъсвания за профилактика са допустими само в кратък интервал.[194]

Структурирането на данните в регистъра е съгласно специално определен за целта стандарт, наречен X.500.[195] Достъпът до регистъра може да е през всякакъв интерфейс - по LDAP протокол[196] или автоматизирано чрез OCSP протокол.[197] Доставчиците без изключение осигуряват достъп и чрез стандартизирано уеб-базирано приложение през HTTP/HTTPS протокол.[198]

Доставчикът на удостоверителни услуги не може да ограничава достъпа до регистъра. Смисълът на регистъра е да е публичен и всички трябва да имат достъп до него. От това правило има изключение. Достъпът може да се ограничава единствено по волята на автора и то само по отношение на удостоверение за неговия публичен ключ. Мотивите на автора могат да бъдат различни. Най-често това се налага при използването на удостоверения са-

---

[192] Арг. от чл. 33 НДДУУРНПИПУУ във връзка с чл. 31 и чл. 32.

[193] Вж. Калайджиев, А., Белазелков, Б., Димитров, Г. и др., *цит. съч.*, стр. 245.

[194] Вж. 39 НДДУУРНПИПУУ.

[195] X.500 е група стандарти за формализирано представяне на структурирани регистри, разработен от ITU-T. Съществува утвърден стандарт на Международната стандартизираща организация – ISO под номер ISO/IEC 9594.

[196] LDAP, Lightweight Directory Access Protocol е формулиран като стандарт от IETF с код RFC 4511.

[197] OSCP, Online Certificate Status Protocol е формулиран като стандарт от IETF с код RFC 2560.

[198] HTTP/HTTPS, Hyper Text Transfer Protocol/Secure е формулиран като стандарт на IETF с код RFC2616.

мо за нуждите на подписване на електронни документи в рамките на дадена общност (например в рамките на една банка или фирма). При въвеждане на такива ограничения, всеки опит за проверка в регистъра за издаденото удостоверение следва да се отказва.[199] Титулярят не може да поиска ограничаване на достъпа. Това е така, защото титулярят е снабден с възможността при прекратяване представителната власт на автора по всяко време да заяви това обстоятелство пред доставчика с искане за прекратяване действието на удостоверението.[200], [201]

Ограничаване на достъпа може да има само по отношение на публикувано удостоверение, но не и по отношение на останалите документи по чл. 28, ал. 3.[202]

Редът за водене на регистъра е уреден с Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги (НДДУУРНПИПУУ).

2.2.4.4.5. Признаване на правната валидност на чуждестранни удостоверения

Електронният свят е неограничен от териториалните граници. Поставя се въпрос признава ли се правната валидност на удостоверения за квалифициран електронен подпис, издадени от чуждестранни доставчици в чужбина на територията на Република България и обратно.

Отговорът на този въпрос се открива в чл. 40 ЗЕДЕП. Той е различен за удостоверения, издадени от ДУУ в ЕС и от други държави.

---

[199] Това се осъществява на практика чрез определянето на специален атрибут в регистъра за ограничение на достъпа до отделно публикувано в регистъра удостоверение.

[200] Арг. от чл. 27, ал. 3, т. 2.

[201] Вж. Калайджиев, А., Белазелков, Б., Димитров, Г. и др., *цит. съч.*, стр. 243.

[202] *Пак там*.

Предвид членството на Република България в ЕС и принципа за свободно движение на стоки, капитали и хора[203], Директива 1999/93/ЕС е създала наднационална рамка, целяща хармонизиране на признаването на трансгранични удостоверителни услуги. В тази връзка съответно транспонираният текст на българския закон установява правилото, че удостоверения за квалифициран електронен подпис, издадени от доставчици на удостоверителни услуги, установени в други държави - членки на ЕС, или в държава - страна по Споразумението за Европейското икономическо пространство, се признават за равностойни на удостоверения, издадени от български доставчик на удостоверителни услуги. Други условности няма.

Поставя се въпросът как се установява дали един доставчик на удостоверителни услуги е „установен“ в друга страна членка на ЕС и как да се обезпечи проверката за валидността на удостоверенията, издадени като такива за квалифициран електронен подпис. Решението е открито в установяването на регистри (списъци) с доставчиците на удостоверителни услуги, които са уведомили националния регулаторен орган, осъществяващ контрол върху дейността на доставчиците в съответната страна членка (в България – КРС). Регистрите трябва да отразяват и статуса на предоставяните от местните доставчици услуги. У нас такъв регистър е създаден с Наредбата за реда и условията за водене, съхраняване и достъп до регистъра на доставчиците на удостоверителни услуги (НРУВСДРДУУ)[204] Страните членки следва да осигурят свързаност на регистрите си по начин, който позволява проверка на статуса на доставчиците и услугите по оперативно съвместим начин. Съгласно чл. 11, ал. 3 НРУВСДРДУУ КРС осигурява този достъп до регистъра във формат, подлежащ на ав-

[203] Чл. 26 ДФЕС.

[204] Приета с Решение № 271 от 10 март 2010 г. на Комисията за регулиране на съобщенията, обн. ДВ бр. 27 от 1 април 2011 г.

томатизирана обработка[205], съобразно изискванията на Решение 2009/767 на Европейската комисията от 16 октомври 2009 г. (изменено с Решение № 425 от 28 юли 2010 г.[206]) за определяне на мерки, улесняващи прилагането на процедури с помощта на електронни средства чрез „единични звена за контакт“ в съответствие с Директива 2006/123/ЕО на Европейския парламент и Съвета относно услугите на вътрешния пазар[207].

Удостоверения за квалифициран електронен подпис, издадени от доставчици на удостоверителни услуги, установени в други държави съгласно националното законодателство на тези държави, не се признават автоматично за равностойни на удостоверения, издадени от български доставчик на удостоверителни услуги.

За тях трябва да е изпълнено някое от следните условия:

1. задълженията на доставчика на удостоверителни услуги, издал удостоверението, и изискванията към неговата дейност трябва да съответстват на изискванията, предвидени в ЗЕДЕП, и доставчикът на удостоверителни услуги да е акредитиран в държава - членка на Европейския съюз, или в държава - страна по Споразумението за Европейското икономическо пространство;

2. доставчик на удостоверителни услуги, установен в държава - членка на Европейския съюз, или в държава - страна по Споразумението за Европейското икономическо пространство, да се е задължил да отговаря за действията и бездействията на установения в друга държава доставчик на удостоверителни услуги в случаите, установени в нашия закон[208], или

---

[205] Вж. Приложението към НРУВСДРДУУ.

[206] OJ L 199/30 от 31 юли 2010 г.

[207] OJ L 299/18 от 14 ноември 2009 г.

[208] Чл. 29 ЗЕДЕП.

3. удостоверението или доставчикът на удостоверителни услуги, издал удостоверението, да е признат съгласно влязъл в сила международен договор между Европейския съюз и трети държави или международни организации или съгласно международен договор между Република България и трета държава.

Условията по т. 1 и 2 се установяват от Комисията за регулиране на съобщенията (КРС) чрез публикуването в отделни списъци във водения от нея регистър на чуждестранните доставчици на удостоверителни услуги, чиито удостоверения са признати при условията на закона и наименованието на поелия отговорността доставчик, както и условията, при които е поета отговорността.

2.2.4.5. Удостоверение за време

Макар да не е задължителна предпоставка за определянето на електронния подпис като квалифициран, удостоверението за време може да придружава квалифицирания електронен подпис и има важни правни последици във връзка с доказването на достоверна дата на подписания електронен документ.

Издаването на удостоверението за време е факултативна услуга, която може да се предоставя, но може и да не се предоставя от доставчика. Това зависи изцяло от неговата пазарна политика, технологична и организационна готовност.

Услугата може да се предоставя само от доставчици на удостоверителни услуги, които издават удостоверения за квалифициран електронен подпис, т.е. които отговарят на изискванията и извършват дейност на доставчик съгласно ЗЕДЕП.[209]

Удостоверението за време е електронен документ, който удостоверява времето на представяне пред доставчика на удостоверителни услуги на електронен подпис, създаден за определен електронен документ. Удостоверението има официална удос-

[209] Арг. от чл. 40 ал. 1 ЗЕДЕП.

товерителна сила. Това означава, че удостоверяването има същата правна сила, както издаването на документ, подписан от орган на властта в кръга на компетенциите му и всички трябва да зачитат удостоверените в него факти до доказване на противното.[210]

Удостоверението за време е подписан от доставчика на удостоверителни услуги с квалифициран електронен подпис електронен документ. То трябва да съдържа реквизити, точно предписани от закона. Липсата им опорочава удостоверението и то загубва удостоверителната си сила. Реквизитите са съобразени с технологичните стандарти, установени за осигуряване на оперативна съвместимост при използването на електронните подписи и са следните:[211] идентификатор на политиката за издаване на удостоверения за време, съдържаща се в наръчника на потребителя на доставчика на удостоверителни услуги, издал удостоверението за време; представения на доставчика електронен подпис на подписания електронен документ; идентификаторите на алгоритмите, използвани за създаването на електронния подпис; времето на представяне на електронния подпис; уникалния идентификационен номер на удостоверението за време; удостоверението за квалифицирания електронен подпис на доставчика на удостоверителни услуги, издал удостоверението за време, или съответна препратка към него.

Официалната удостоверителна сила удостоверението за време придобива не след издаването му, а едва след вписването му в официалния X.500 регистър на удостоверенията, воден от доставчика.[212] Воденето и съхраняването на удостоверенията за време в регистъра се определят с НРУВСДРДУУ.

Доставчикът на удостоверителни услуги е длъжен да пуб-

---

[210] Относно удостоверителната сила на официалните документи вж. Сталев, Ж., Българско гражданско процесуално право , *цит. съч.*, стр. 275.

[211] Вж. стандарти ETSI TS 101 862 V1.3.1 (2004-03) - Qualified Certificate Profile и ETSI TS 102 280 V1.1.1 (2004-03) X.509 V.3 - Certificate Profile for Certificates Issued to Natural Persons.

[212] Вж. раздел 2.2.4.4.4, *по-горе*.

ликува в регистъра и следната информация, приложима към удостоверенията за време: условията и реда за издаване на удостоверение за време, включително за правилата за установяване идентичността на титуляря на квалифицирания електронен подпис; процедурите за сигурност на доставчика на удостоверителни услуги; условията за достъп до удостоверението за време и начина на проверка на валидността му; цената за получаване и използване на удостоверение за време; отговорността на доставчика на удостоверителни услуги; условията и реда, по които авторът, съответно титулярят прави искане за прекратяване действието на удостоверението за време.[213]

Изискванията към удостоверенията за време, формата и правилата за тяхното издаване се определят с НДДУУРНПИПУУ.