ЕЛЕКТРОНЕН ПОДПИС

1. Същност на електронния подпис.

Съществен елемент на всеки документ е подписа. Неговото използване цели да гарантира истинността и целостта на документа, както и авторството на волеизявленията, извършени в него.

Развитието на съвременните средства за документооборот, на новите платежни системи е немислимо без надеждни средства за обезпечаване автентичността и целостта на документите.

В усилията за създаване на международна, общоевропейска правна рамка , както и в националните законодателства на отделните страни, ключов въпрос като гаранция за правно валидно и надеждно осъществяване на електронния обмен на данни е използването на електронен подпис като средство за създаване на сигурност и доверие в електронната търговия и обмена на данни в откритите мрежи изобщо. Той позволява да се определи от кого произхождат данните , както и да се провери дали те не са променяни , дали не е била нарушена тяхната цялост. С неговото използване се цели да се гарантира истинността и целостта на документа , както и авторството на волеизявленията , извършени в него.

Електронният подпис може да бъде определен като : **реквизит на електронния документ , представляващ сбор от данни в електронен вид (знаци,букви , числа и други символи) , внедрени или функционално свързани с електронния документ с намерение за автентификация на същия.**

Като правна възможност за защита на взаимоотношенията в глобалната мрежа, електронният подпис съхранява редица от свойствата на обичайния собственоръчен подпис. На практика използването му защитава електронния документ от редица действия, като:

- отказ на волеизявителя от авторство;
- модификация на вече потвърден документ;
- подправяне на документ;
- прихващане на данните в момента на техния обмен и модифицирането им и др.

Така въведеното оределение очертава два логически признака на електронния подпис:

- предметен – електронният подпис представлява данни в електронна форма, присъединени или логически асоциирани към други данни;
- функционален – с помощта на електронния подпис се автентифицират данни.

При разглеждането на същността и правната уредба на електронния подпис не можем да отделим чисто юридически или чисто правни характеристики. Тяхната взаимна обвързаност е основна черта на електронните подписи. Затова и в законодателната уредба съществуват редица технически правила , във връзка с механизмите за създаване и проверка на електронните подписи. От друга страна проблемът за правното регулиране на отношенията, свързани с електронната търговия и с използването на електронните подписи, е свързан с регулирането на използваните технологии.

Съществуват редица технически решения за подобряване нивата на сигурност в мрежата. Сред най-често използваните за гарантиране защитата на предаваната информация са протоколите за сигурност – SSL и SET [1]

[1] Възможностти за развитие на електронен бизнес в България, изд.”Агенция Икономика”ЕООД, С. , 2002г.

- **SSL (Secure Sockets Layer**) е защитна система за обмен на данни. SSL криптира обменяните данни и не допуска те да бъдат прочетени от неупълномощени лица. Когато потребителят е в режим на SSL , на най-долния ред на браузера се появява знак – жълт катинар (или ключ) . Сървърите с режим на SSL са с адрес започващ с https: //.

Протоколът SSL осъществява следните функции:

1. Конфиденциалност на връзката – след предварителния диалог между страните се определя секретен ключ , който се използва за симетрична криптография.
2. Идентификация – страните се идентифицират една друга с помощта на асиметрични криптографски методи.
3. Обезпечение на надежността на връзката.

Конфиденциалността на съобщенията се осигурява посредством приемане на комбинирана схема с използване на криптография с открит и симетричен ключ.

- **SET** представлява техническа спецификация за осигуряване предаването на поверителна информация по открити мрежи, каквато е Интернет. Изработена е през 1996г. SET включва :

1. Цялостност – информацията за сметките на клиентите може да бъде предавана по обществените мрежи , без да има промени и загуби при преноса и съхраняването , тъй като използва строго кодиране.
2. Конфиденциалност – показва само необходимата за всеки участник в транзакцията информация.
3. Стандартизираност – SET стандартът дефинира всички необходими процеси – движението на транзакцията , формата на съобщенията , идентифицирането и алгоритмите на кодиране.
4. Неотменяемост – SET стандартът дефинира PKI (Public Key Infrastructure – инфраструктура на публичния ключ) , която се използва за проверка на участниците в транзакцията и за кодиране / декодиране на обменяните съобщения. Участниците се идентифицират със своя цифров подпис , гарантиращ неотхвърляне на сделката.

SET е създаден да осигури конфиденциален начин за плащане и поръчване на стоки и услуги. Цялата информация се кодира. Интегритетът на предаваните данни се осигурява чрез цифров код , който се прилага към всяко съобщение и дава възможност на получателя да провери дали съобщението не е било променено по време на преноса. Използването на цифрови сертификати дава възможност да се удостовери дали ползвателят на картата е нейния легитимен собственик.

Електронният подпис се основава на технологии за автентификация , на системи за криптиране и декодиране. Съществуват няколко методи за създаване на електронен подпис:

- шифроване на електронния документ върху основата на симетричен алгоритъм

-използване на асиметричен алгоритъм за шифроване

- обработка на документа посредством хеш-функция и зашифроване на окончателния резултат с помощта на асиметричен алгоритъм.

Независимо от конкретните методи за осъществяване на електронните подписи обаче , те трябва да са технологично неутрални.

Кодирането / шифрирането/ на данни позволява да се запазва важна информация или да се предава през несигурна мрежа (като Интернет) , така че да не стане достояние на друг освен на получателя, за когото е предназначена. Методът за превръщане на ясен текст така , че да се скрие съдържанието му , се нарича шифроване. Резултатът от шифрования ясен текст в невъзможни за прочитане безсмислици е шифровият текст. Дешифрирането е процесът на превръщане на шифровия текст обратно в оригинален ясен текст. Шифрографията (Criptography) е наука за използването на математиката за шифриране и дешифриране на данни.

Шифрографският алгоритъм или шифър (код) е математическа функция , използвана в процеса на шифриране и дешифриране.[2] Шифрографският алгоритъм работи в комбинация с ключ – дума , цифра или фраза за шифроване на ясен текст. Сигурността на шифрованата информация зависи изцяло от силата на шифрографския алгоритъм и секретността на ключа (кода).

Симетричната (конвенционална) шифрография , наричана още секретен или симетричен ключ за шифроване работи с един ключ за кодиране и за декодиране на информацията, което не удовлетворява необходимата степен на защита на информацията .

Най – често използвана е асиметричната система за криптиране на данни , основана на двойния ключ – публичен и частен. Частният ключ се използва за генериране и кодиране на електронния подпис посредством алгоритъм. Достъп до него има само лицето , което създава електронно подписания документ. Частният ключ е свързан със съответен публичен ключ– публично достъпен код , с помощта на който адресатът на електронното съобщение може да разчете кодираното съобщение и да удостовери автентичността на електронния документ и ненакърнеността на съдържанието му.

Кодът е инструментът , който работи с шифровия алгоритъм за получаване на специфичен шифротекст. Кодовете принципно са много големи цифри. Размерът на кода при асиметричната система на кодиране и конвенционалното шифроване е абсолютно несъвместим. Пример : конвенционалният 80 – байтов код има еквивалентна сила на 1024 – байтовия публичен код.

В някои случаи в практиката се използва фибридна шифросистема , която е комбинация между двата шифроващи метода и включва сигурността и удобството на публичния код с бързината на конвенционалното шифроване.

Асиметричната система за кодиране е основният възприет метод за създаване на цифрови подписи.Те позволяват на получателя на информацията да установи автентичността й, а също така да потвърди, че информацията е чиста.

В основата на математическото определение но електронен цифров подпис стои понятието “ едностранна функция със секрет”, въведена през 1975г. от американските математици У. Диффи(W.Diffie) и М.Е. Хелман(M.Hellman).[3] Едностранната функция се нарича функция F , на която са присъщи следните свойства:

1. за всеки секретен ключ **к** и всеки подпис **s** значението на функцията **F** може да се изчисли достатъчно просто , при което за изчисление по известно **s** на значението на съобщението **m** не е задължително знаенето на ключа **к;**

[2] An Introduction to Criptography by Philip Zimmerman , Network Associates ,Inc http:// www.nai.com.

[3] Правовые аспекты использования Интернет – технологий, Книжный мир ,2002.

2. ако секретният ключ **к** е неизвестен , то по известно **s** (подпис) и **m** (съобщение) е невъзможно лесно да се намери ключа **к**;
3. ако секретният ключ **к** е известен , то по известно зададено **m** може лесно да се изчисли **s.**

Използването на едностранната функция за системата електронен цифров подпис се основава върху това , че документът подписан с електронен подпис, се разглежда като числа **m** и **s** , където **m** е съобщение (например някаква информация в електронна форма) , а **s** - подпис , получен по пътя на решение на уравнението **F (k,s) =m** , в което **F** - е известната на всички участници в електронния документооборот едностранна функция, а **к** е секретният ключ.

Знаейки секретният ключ , неговият притежател може по всяко време да подпише даден документ , а доколкото публичният ключ (функцията F) е известен на всички ползватели на информационната система , то всеки от тях може да провери автентичността на подписа. При това , който и да е , не знаещ частния ключ не може да изчисли **к** или да подпише електронния документ. В случай на изтичане на информация при предаването на данните по каналите за връзка значението на електронния цифров подпис се изменя и той става недействителен.

Доколкото обемът на предаваните електронни документи може да бъде достатъчно голям , то на практика , за да не се оперира с големи числа, подписът се изчислява не за самото съобщение **m** ,а за някакво число , получено посредством прилагането спрямо него на специална функция , наречена хеш – функция. Това е алгоритъм , който превежда една последователност от битове в друга, по – малка(хеш резултат) , по такъв начин , че :

- записът дава един и същ хеш резултат всеки път, когато алгоритъмът се използва при въвеждане на същия запис;
- невъзможно е чрез изчисляване записът да бъде извлечен и реконструиран от хеш резултата , произведен от алгоритъма;
- невъзможно е чрез изчисления да се стигне до два записа, които водят до един и същ хеш резултат при използването на алгоритъма;

Хеш – значението на документа – това е контролната сума , изчислена с помощта на хеш – функцията , така че хеш – значението на всеки документ е уникално. При внасянето на най – малкото изменение на документа (дори с един файл) неговото хеш – значение се променя.

От техническа гледна точка електронният подпис изглежда като хеш – значение на документа , изчислено с помощта на определен известен алгоритъм и зашифрован частен ключ на подаващия данни в системата , при това електронният подпис трябва да съдържа указания за метода на изчисляване на хеш – значението , т.е. хеш – функцията.

Така получателят на документа може с помощта на публичния ключ на отправящия да разшифрова хеш – значението, указано от отправящия и да го сравни с фактическото хеш – значение на получения документ. Ако те съвпадат , то това е гаранция , че документът е бил подписан от притежателя на частния ключ и че в процеса на предаване на документа в него не са направени изменения. Тези операции се извършват със специални програми (Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис (ПМС №17 от 2002г.; ДВ.,бр.15 от 8 февруари 2002г.)[4]

[4] Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис (ПМС №17 от2002г.;обн.,ДВ,бр.15 от 8 февруари 2002г.).

С оглед спецификата на разглежданата тематика е необходимо да направим и някои уточнения по отношение на най- често употребяваните термини, свързани с функциите на електронния подпис.

1. **Автентификация** – често електронния подпис се определя като автентифициращо средство и дори се отъждествява с него. (виж долу). Най- често когато за неговото създаване не се предвижда нито конкретна технология, нито специална процедура(пр. Издаване на удостоверение) и може да бъде уговорено между страните. С автентификация функции се свързва т. нар. обикновен подпис.

Автентификацията на ЕД придава правната форма , която гарантира негоовата достоверност (традиционен ддокументооборот – аналог подписан документ) от гледна точка на връзката на конкретно лице с конкретен подпис и съгласието на това лице с подписаното изявление (отъждествяване на това лице със съдържанието на документа).

Автентификацията посредством използването на електронен подпис се осъществява на основата на : веществен признак – идентифициращото средство е определена вещ, която принадлежи на ползвателя (удостоверение за частен ключ, смарт – карта и т. н.). Възможна е автентификация по запомнящ се признак, на основата на информация, известна на ползвателя(еднократна или мнагакратна парола, кодова фраза, персонален идентификатор и др.) или личен признак, на основата на характеристики, зависещи от физическите свойства или качества на ползвателя(биометрични характеристики) към които се отнасят отпечатъци от палци, снимка на очната ретина, биометрия на гласа и т. н.

Във всички случаи идентифициращото средство, установява, че конкретно лице е негов ползвател, но това не означава a priori, че документа изявлението е автентифицирано, защото връзката на резултата от автентификацията не е с конкретно лице, а със съответно идентифициращо това лице средство. Възможно е идентификаторът да бъде откраднат , загубен и несанкционирано използван.

Затова правото създава различни регулаторни механизми (използването на определени алгоритми, удостоверяване на електронните подписи и пр.), които да създадат по- голяма степен на сигурност, с оглед конфиденциалността и целостта на информацията.

2. **Конфиденциалност** – само по себе си идентифициращото средство, което може да изпълнява функциите на електронен подпис, (когато закона не предвижда ограничения или специфични изисквания за неговото създаване и проверка), не винаги гарантира конфиденциалността на данните. Това се постига посредством използване на шифрографски алгоритми (симетрично криптиране, асиметрично криптиране и най-често използваната хибридна система (Наредба) Електронният подпис се основава на технологии за автентификация, на системи за криптиране и декодиране. Най- често използвана е асиметричната система за криптиране на данни, основана на двойния ключ – публичен и частен. Частният ключ се използва за генериране и кодиране на електронния подпис посредством алгоритъм. Достъпът до него има само лицето, което създава електронно подписания документ. Частният ключ е свързан със съответен публичен ключ – публично достъпен код, с помощта на който адресатът на електронното съобщение може да разчете кодираното съобщение и да удостовери автентичността на електронния документ и ненакърнеността на съдържанието му.

Конфдиденциалността гарантира това, че лице, което няма съответните права, не може да има достъп до информацията, предавана в рамките на транзакцията.

Важно е да се отбележи, че електронен подпис не е тъждествен на шифроване. Не всеки шифрован текст е подпис и не всеки подпис трябва да е създаден с методите на шифрографията. Правните норми установяват осовеностите на използване на една

или друга технология и възможните варианти за съчетаване с оглед нуждите на оборота и целесъобразността.

3. Цялостност – осигурянето и посредством електронен подпис е гаранция за това, че транзакцията не е подправена. Отграничаването на съдържанието на термина от разгледаните други по- горе е необходимо от гледна точка на регулирането на използваните средства.

Функцията по осигуряване целостта на данните се постига посредством използването на специална математическа функция – хеш- функция. Посредством използването и от изходния текст на съобщението се получава негов съкратен фрагмент – дайджест съобщение(message digest) или хеш код (hash code). Към този фрагмент се прилага криптографическо преобразуване чрез използването на частен ключ за подписване и открит ключ за проверка на електронния подпис.Следствие от използването на хеш функцията при внасянето и на най- малко изменение в документа(дори с един файл) неговото хеш- значение се променя. (Наредба за алгоритмите за създаване на електронен подпис)

Тази особеност в предмета на регулиране предпоставя създаването на йерархични модели, където условията за признаване на действителност се изменят в зависимост от вида на конкретния електронен подпис и сертификата. В едни случаи страните могат сами да избират начина на автентифицирани на волеизявленията , в други да използват конкретна процедура за подписване, съобразена със законовите изисквания за съответния вид подпис.

В зависимост от степента на защита, както и от сверата на употреба, на електронните подписи (публична, частна), и на издаваните към тях удостоверения (ако са предвидени такива),се предявяват редица специални изисквания и се предвиждат определени правни последици. Тези последици могат да бъдат ограничени до определен кръг правоотношения, или обвързани с допълнително изисквания.За индивидуализиране на отделните видове електронни подписи и сертификати се използват допълнително квалификации. Директива 1999/93 /ЕС въвежда понятията “усъвършенстван електронен подпис” (advancad electronic signature), “ квалифициран сертификат” (qualified certificate), “защитен механизъм за създаване на подписа”(secure signature creation device). Българският законодател работи с понятията “усъвършенстван”, “универсален” електронен подпис, “ регистриран доставчик на удостоверителни услуги”.

Следва да отбележим, че понятията “електронен подпис” , и“ цифров подпис” са идентични. Определението “ цифров” обикновено се свързва с технологичната природа на подписа (цифрова форма , цифрово изявление).

Юридическите признаци на електронния подпис се различават от техническите, описани по – горе , тъй като правните норми могат да въведат както ограничения в използването на определени видове електронен подпис , така и да установят допълнително гаранции за тяхната достоверност в интерес на участниците в документооборота. Проблемът за правното регулиране на отношенията ,свързани с електронната търговия и с използването на електронните подписи, е свързан с регулирането на използваните технологии.

От гледна точка на правото е важно технологията , която се използва , да съответства на целите , за които се използва.

Правотворческите органи решават доколко един или друг технически способ за документооборот е надежден , каква е вероятността от изопачаване на волята на страните в електронния документ , кой притежава правото да реши във всеки конкретен случай въпроса за автентичността и въз основа на какви критерии.

Като правна категория цифровият подпис съществува чрез своите юридически признаци , закрепени в нормите на правото.

Съществуват два подхода към определянето на електронния цифров подпис като правна категория. Тази неоднозначност е предопределена от сравнително малкото практика в тази насока и от традиционализма на правните системи.

Според единия подход електронният цифров подпис е аналог на собственоръчния подпис и при спазване на посочените в закона условия придобива тъждествена със собственоръчния подпис юридическа сила. Другият подход не придава адекватна юридическа сила и доказателствена стойност на двата вида подписи.[5] Съответствеността на електронния цифров подпис и собственоръчния подпис се основава на удостоверителните функции , които те изпълняват .

Доколкото и електронният цифров подпис и собственоръчният подпис се използват за автентификация на авторството на документите , то те се разглеждат като аналогични. Но характерът на връзката между автора на документа и създадения от него електронен цифров подпис принципно се отличава от характера на връзката между автора и неговия собственоръчен подпис. За разлика от собственоръчния подпис , носещ в себе си информацията за индивидуалните признаци на автора , електронният цифров подпис позволява да се установи само факта на неговото създаване с помощта на частния ключ. Изводът за тъждеството на автора на документа с притежателя на частния ключ е основан върху предположението , че секретния ключ е известен изключително на неговия притежател. Авторите отбелязват , че по указаните по – горе причини електронният цифров подпис не може да бъде определен в нормите като юридически равнозначен на собственоръчния , защото това ще доведе до объркване на участниците в правоотношението и ще породи процесуални трудности при идентификацията на лицата, използващи електронен цифров подпис за заверка на компютърни документи. В защита на своята теза авторите привеждат и допълнително аргументи. Те смятат , че ако се приеме като изходно положение юридическата тъждественост между електронния цифров подпис и собственоръчния подпис , това би довело до погрешно решение на редица правни проблеми, като :

- има ли право притежателя на частния ключ да приведе доказателства в потвърждение на това , че той не е автор на документа, подписан с електронен цифров подпис , ако достоверността на подписа е била удостоверена;
- смята ли се договорът за сключен , ако автентичността на електронния цифров подпис е потвърдена , но собственикът на секретния ключ не е автор на документа;
- кой в този случай носи риска от вредите. [6]

Според същите автори притежателят на ключа не би могъл да оспори авторството , тъй като електронният цифров подпис е юридически приравнен със собственоръчния , автентичността на който е била надлежно установена. Следователно , фактът на сключване на договора , подписан с електронен цифров

[5] Вж. Правовые аспекты использования Интернет- технологий, цит.съч., с. 106-108.
[6] Пак там.

подпис, не може да се оспори на основание на това, че притежателят на частния ключ не е автор на документа .

Посоченият подход по принцип поставя някои от проблемите, свързани с използването на електронните подписи , но много от тях не са изключително свързани с правоотношенията в киберпространството . Те са законодателно решени и не се нуждаят от допълнително нормативно обвързване.

Мислим обаче за необосновано твърдението, че доказването на автентичността на електронния цифров подпис е доказване *a priori* авторството на подписания документ.

Това би ограничило възможността за оспорване на авторство и доказване , че даден документ е бил променен така ,че неговото съдържание се отличава от това , което е било подписано и волеизявлението на автора е било частично или изцяло променено.

Притежателят на частния ключ може на същите правни основания , каквито има положилият собственоръчен подпис, да оспори или потвърди авторството върху подписания документ. Противното би създало несигурност на документооборота в мрежата , както и ако правото не признае юридическа сила на електронния цифров подпис с правни последици, адекватни на тези, произтичащи от полагане на собственоръчен подпис.

Съществува разлика и тя е по – скоро техническа в начина на доказване на автентичността на двата вида подписи. При собственоръчния подпис доказването е съпроводено от графологична експертиза , която потвърждава или отхвърля биологичната връзка между подписващото лице и положения подпис . При електронния цифров подпис съществуващата презумпцията , че притежателят на частния ключ е подписалото документа лице, може да бъде оспорена, като се докаже , че ключът (кодът) е бил узнат и използван неправомерно.

Редица от поставените въпроси намират законодателно решение в създадените международна , общоевропейска правни системи, и в националните законодателства на отделните страни, като се гарантира сигурността и защитата на транзакциите и взаимоотношенията , осъществявани по електронен път. При подхода към тези актове се предвижда , че те трябва да си приличат , макар и само в основните принципи, поради универсалността на решаваните задачи.

Следователно е необходимо да се намери баланса между националните традиции на законодателстване и необходимостта от унификация на правните норми , тъй като автономното прилагане на специфично национално законодателство ограничава възможностите на една страна за участие в глобалния пазар. В този аспект трябва да се отбележи , че отношенията, свързани с мрежата, предизвикват *две нива* на регулирането им –национално и международно.

2. Международна система на регулиране.

В *международната система* трябва да се отграничат две подсистеми: система на ООН и актове на ЕС .

В системата на ООН работата по правното регулиране на отношенията в областта на електронната търговия е съсредоточена в Комисията по международно търговско право – UNCITRAL. През 1996г.от тази Комисия са разработени Закон – модел за електронна търговия (MLEC) и Закон – модел за електронния подпис (MLES)– от 2000г .[7] В тях се признава юридически статус на

[7] http:// www.unictral.org/english/documents.

електронните документи , премахват се юридическите бариери за използването на електронни споразумения , отменя се “монопола на книжните документи”

Законът – модел за електронна търговия , приет с резолюция на Генералната Асамблея на ООН №ООН А /51/628 от 16 дек. 1996г. , визира , че ако съответното законодателство изисква наличието на подпис на лицето върху съответния документ , то това изискване се смята за изпълнено ако :

- е използван какъвто и да е било способ за идентификация на лицето , че това лице е съгласно с информацията , съдържаща се в съобщените данни;
- този способ да е както надежден , така и съответстващ на целите за които съобщението на данните е било подготвено или предадено , с отчитането на всички обстоятелства , включително и всички съответстващи договорености.

Дадената формула в действителност е много обща , тъй като не установява критериите за оценка на съответствието на метода с изредените в нея изисквания. Съответно , не могат да се дадат и по – нататъшни гаранции за юридическата сила на информацията в електронен вид.

Отговор на някои от въпросите дава Законът – модел за електронните подписи /MLES/ от2000г. Структурно документът се състои от три части : (1) критерии за надеждност и достоверност на електронните подписи; (2) обвързаността на страните по правоотношението , свързано с използването на електронните подписи; (3) признаване на подписа в чужда държава;

В закона са формулирани стандартните изисквания към електронния подпис и условията, при които на конкретен подпис , поставен под конкретен документ може да бъде призната юридическа сила:

- данните, представляващи електронен подпис , трябва да бъдат непосредствено свързани с лицето , подписващо документа, т.е. подписът да изключва неяснота за това, кой го е поставил;
- подписването , в момента когато то се извършва , да бъде под контрола единствено на подписващото лице; предполага се , че лицето само , изразявайки своята воля ,подписва документа и никой не може да постави неговия подпис без негово знание; ако някой действа от името на друго лице , се прилагат общите правила за представителството;
- всяко изменение на електронния подпис , направено след подписването може да бъде разкрито;
- ако законът изисква целостта на подписания документ да бъде потвърдена с подпис , всяко изменение в него , направено след подписването , може да бъде разкрито.

Въпросът с потвърждаването на автентичността на подписа въвежда към проблема, свързан с интернационалния характер на компютърната мрежа. Ще има ли подписът , сертифициран в една държава, същата призната юридическа сила в друга държава. Законът решава този проблем ,като установява общо правило – чуждестранният подпис се признава в страната на получателя на подписания документ. Подписът с чужд произход трябва да има същата юридическа сила , ако технологиите на подписването са еквивалентни по същество(sustantially equivalent) в страната на получателя, при установени общи критерии за еквивалентност. За признаването на чуждестранен подпис е необходимо убеждението за това ,че при неговото създаване са използвани такива методи ,

които са възприети при създаването на подписа в признаващата държава, като под това се разбират не определени технически стандарти , а общите принципи при създаването на даден електронен подпис.

Впрочем тази процедура е описана доста неясно и е неефективна , тъй като би затруднила международната търговия. Тя е твърде абстрактно описана, за да може реално да обслужва търговските взаимоотношения, поради това е трудно да бъде възприета и приложена в практиката.

Различен от този общ и принципен подход се следва в Директива 1999/93/ЕС на Европейския парламент и Съвета на Европейския съюз от 13 декември 1999г., относно рамката на Общността върху електронните подписи , в сила от 20 яннуари 2000г.(Electronic Signatures Directive).[8] По своето съдържание тя напомня MLES (на UNCITRAL),но структурно има известни различия. MLES обръща основно внимание на проблема за действителността на подписите и правата и отговорностите на страните. Актът обобщава натрупаната практика в областта на сключването на електронни сделки и създава единни и ясни критерии за признаване на чуждестранен електронен подпис. Директивите са законодателен инструмент , използван от ЕС. В тях се съдържа задължителния резултат , който държавите – членки са длъжни да постигнат в установен срок, при което формите и методите за постигането на този резултат са оставени на свободната преценка на самите държави.

Директивата дава следното решение на въпроса за тъждествеността на подписите : стриктно изброява случаите , когато е възможно признаването на чуждестранен електронен подпис , вместо възприемането на принципа за еквивалентност на технологията на подписване по същество . Възможностите за признаване са изброени както следва :

- на взаимна основа се признават подписите , създадени в държавите– членки на ЕС , доколкото те се основават на общите изисквания на Директивата.
- ако подписът е създаден в държава,която не е член на ЕС , но съответства на изискванията на Директивата , може да бъде признат в държава , която е член на ЕС ; в този случай могат да се установят допълнително изисквания към подписите;
- за признаването на подписите могат да се сключват двустранни и многостранни споразумения между държавите; за Еврокомисията остава правото да регулира въпросите за унификация на техническите стандарти, за отстраняване на необосновани препятствия в международната търговия.

Не възниква съмнение, че подходът, възприет от Еврообществото е по-точен и строг от този, предлаган в Закона – модел за електронните подписи на UNCITRAL. Установяването на единни критерии, на които трябва да съответства електронния подпис, спомага за укрепването на единно правно и икономическо пространство в Европейското общество и осигурява допълнителни гаранции за безопасността на използваните технологии.

Трябва да се отбележи , че Директива 1999/93/ЕС е сред най- важните международни инструменти в рамките на ЕС през последните години , отнасящи

[8] Directive 1999/93/EC of the European Parliament and of the Conncil of 13 December 1999 on a Community Framework for Electronic Signatures//Official Journal of the European Communities LO 13, 19.01.00,p12.http://europa.eu.int/comm/dg 15/en/media/sign/elecsignen.pdf.

се до използването на електронните подписи. Този нормативен акт дава основните насоки за регулация и хармонизиране на законодателството в страните от Европейската общност по отношение на електронните документи и електронните подписи без да навлиза в националните норми на договорното право.Целта на изискванията , заложени в нея, се състои в гарантиране на това , че е достигната максимална степен на безопасност на електронния документ и свързания с него електронен подпис. Разпоредбите й относно правната сила на електронните подписи не накърняват изискванията към формата , възприети в националните законодателства относно сключването на договора и правилата, определящи дали договорът е бил сключен.

Електронният подпис е дефиниран като (обикновен) електронен подпис или "несигурен", и "усъвършенстван" или (сигурен) електронен подпис .[9] Това разграничаване е обусловено от различните технически изисквания , осигуряващи различна степен на обезпеченост на съответния електронен подпис и заедно с това различният правен режим, даващ възможност на страните да възприемат в своите национални законодателства най- подходящия вариант в съответствие с техните правни системи.

Електронен подпис (electronic signature) е определен като информация в електронна форма , придружена или логически свързана с друга електронна информация и служеща като средство за автентификация. Това е т.нар. "обикновен електронен подпис"- обикновен , защото законодателят не обвързва създаването и използването му с изисквания от технологичен характер , нито с други допълнителни условия. Той може да бъде създаден и възприет от страните в правоотношението при пълна свобода да договарят помежду си начина на авнентифициране на електронното изявление.

Правното действие на електронния подпис се признава на основание на електронна форма , като допустимостта му в качеството на доказателство в процеса не може да бъде отказано на нито едно от следните основания :

- че подписът е в електронна форма ;
- е основан на квалифицирано удостоверение;
- не е основан на квалифицирано удостоверение , издадено от упълномощен доставчик на удостоверителни услуги; или
- не е създаден чрез защитен механизъм за създаване на подпис.

Много по- строг режим е въведен за **Усъвършенствания електронен подпис (advanced electronic signature)** – това е електронен подпис , който отговаря на следните изисквания :

1. свързан е по уникален начин с подписващото лице;
2. способен е да идентифицира подписващото лице;
3. създаден е със средства , които подписващото лице държи единствено под свой контрол;
4. свързан е с информацията по такъв начин , че всяка последваща промяна в нея може да бъде открита.

Така определен, електронният подпис визира високата степен на защита , която е нужно да осигури по отношение на данните, предавани по електронен път. Това е необходимо и поради факта , че на електронния подпис се признава същата правна сила по отношение на електронните данни , каквато притежава саморъчният подпис по отношение на хартиения носител и има същата доказателствена сила в съдебния процес.

[9] Вж.Димитров,Г.Режим и практическо приложение на електронните подписи-Обикновен електронен подпис.-В: Пазар и право, кн. 1,2003г.

С цел да се улесни на електронната търговия усъвършенстваният електронен подпис се приема като доказателство по всеки въпрос , свързан с автентификацията и ненакърнеността на комуникацията или данните и се ползва със същата правна сила в процеса като саморъчния подпис. За да бъде обаче признат за правно еквивалентен на саморъчния подпис и да има еднаква правна сила по отношение на електронните данни, каквато има саморъчният подпис спрямо хартиения носител, Усъвършенстваният електронен подпис трябва да се основава на « квалифицирано удостоверение» (определено и отговарящо на изисквания посочени в текста и Приложенията на Директивата) и да бъде създаден чрез « защитен механизъм» за създаване на подписи. Той ще има същата доказателствена сила в съдебния процес при условие , че изискванията за саморъчните подписи са спазени.

Придадената юридическа сила на Усъвършенствания електронния подпис задължава по отношение на механизмите (техническите и процедурните средства), използвани за неговото създаване и използване.Те трябва да гарантират, че данните , използвани за създаване на подписа и неговото генериране :

- да могат практически да се възпроизвеждат само веднъж и тяхната сигурност да бъде надеждно защитена;
- да не могат с достатъчна сигурност да бъдат извлечени и подписът да е защитен срещу подправяне чрез използване на наличната сега технология;
- да могат да бъдат надеждно защитени от легитимното подписващо лице срещу използването им от други лица.

Тези съображения за сигурност обуславят необходимоста от система за кодиране , при която да има възможност закодираният документ да се декодира без в него да могат да се внасят последващи промени (за системите за кодиране стана дума по- горе).

Въпреки наличието на определения и специални изисквания за сигурност, текстът на Директива 1999/93 на ЕС остава технологически неутрален – единственото изискване се състои в това да се гарантира достигане на максимална безопасност , вместо указания за конкретно устройство или метод на създаване на електронния подпис.

3. Регулиране от националното законодателство.

Второто ниво на регулиране на електронния обмен на данни и в частност на електронните подписи е националното законодателство. Докато международните актове очертават абстрактният модел на осъществяване на взаимоотношенията в електронното пространство и визират общите рамки на тяхното развитие като една виртуална възможност, националните норми конкретизират реализацията на тази възможност.

Определенията, дадени в Директивата са възприети в повечето държави в Европа.

Концептуалните основи на регулирането на правоотношенията , осъществявани по електронен път и в частност придаването на юридическа сила на на предаваните по електронен път изявления и извършваните посредством тях правно валидни действия се съдържат в Закона за електронния документ и електронния подпис (ЗЕДЕП) , приет на 22 март 2001г. (ДВ, бр.34 ,2001г), в сила от 06.10.2001г . Това е първата стъпка към осъвременяване на българското законодателството в съответствие с новите изисквания на икономическите процеси и променената бизнес среда.

ЗЕДЕП е типичен континентален закон в областта на регулирането на електронния документ и електронния подпис , където на първо място е поставена безопасността на документооборота и публичната достоверност на подписите , за което се предвиждат задължителни процедури за създаване на електронни цифрови подписи , издаване на удостоверения от доставчици на удостоверителни услуги , въвеждане на регистър наудостоверенията.

Проблемите, които ЗЕДЕП решава са свързани основно с идентификацията на страните в търговските правоотношения, правната сила на електронното изявление и електронния документ, като правно валидна форма за осъществяване на електронни сделки.

Законът урежда правния статут на електронния документ и електронния подпис , като при подготовката на текстовете са следвани предписанията на Директива 1999/93/ЕС , на модел за Закон за цифровия подпис (1996г.) изготвен от Комисията по търговия и законодателство към ООН (УНСИТРАЛ) , както и успешно прилаганите вече законодателни решения в други страни. Във връзка с прилагането на закона МС приема няколко наредби.

Въпреки, че ЗЕДЕП възприема в голяма част принципите , заложени в Директива 1999/93, законодателят подхожда самостоятелно към регулираните проблеми , отчитайки спецификите на икономическите процеси в страната и националните правни традиции .

Законодателят изгражда правната уредба на електронния подпис като използва йерархичния модел, на основата на два принципа:

- технология и инфраструктура на електронните подписи;
- сфера на приложение.

В частно правните отношения, със значението на саморъчни подписи могат да се използват – “ електронен подпис” (обикновен), и “ усъвършенстван електронен подпис”(чл.13 (1)т.1 и т.2ЗЕДЕП), а в публичната сфера правно валидно действие има използването на “ универсален електронен подпис”(чл.13,ал.1,т.3ЗЕДЕП), който се прилага и в отношенията между частни лица и публични субекти (държавен орган или орган на местно самоуправление). Универсалният електронен подпис има значението на саморъчен по отношение на всички.(чл.13,ал.3).

Изготвения първоначално на експертно ниво Проект за Закон за електронния подпис, стои по- близо до определенията дадени в Директивата . С понятието “ автентификация” е дефиниран “обикновения подпис” по смисъла на Директивата на ЕС , а с “електронен подпис”- “усъвършенстваният”

“ Автентификацията на електронното изявление разкрива самоличността на автора и съгласието му с електронното изявление” – определението дава пълна свобода на страните в правоотношението да уговарят помежду си начина на автентифициране на електронното изявление – това може да бъде както чрез електронен подпис , така и по всякой друг начин , възприет от тях , стига той да бъде достатъчно сигурен с оглед нуждите на оборота.

По- нататък в Проекта електронния подпис е определен като : “Преобразувано електронно изявление , включено , добавено или логически свързано със същото електронно изявление преди преобразуването”.

На електронния подпис е признато значението на правно валиден подпис , с което се признава неговата юридическа сила и допустимостта му като доказателство в процеса , което не се гарантира на автентифициращото средство , т. е. на обикновения електронен подпис.Тези положения не кореспондират с принципа възприет в Директивата на ЕС за признаване на правно действие на електронния документ и електронния подпис само на основание на това , че са извършени в електронна форма.

В Проектозакона , внесен за разглеждане и гласуване от НС , формулирането на понятието “ електронен подпис”и свързаните с него правнорелевантни последици, е различно от първоначалните законодателни намерения и така предложените текстове съставят окончателния вариант на Закона за електронния документ и електронния подпис.

Законът подхожда сравнително строго към електронния подпис като автентифициращ елемент , пряко свързан с електронното изявление. Придаването на правна сила на обикновения електронен подпис е за сметка на диспозитивния характер на нормите, които го уреждат.

Електроннният подпис е определен в чл.13,ал.1,т.1ЗЕДЕП като – всяка информация , свързана с електронното изявление по начин , съгласуван между автора и адресата , достатъчно сигурен с оглед нуждите на оборота ,който:

-разкрива самоличността на автора;

-разкрива съгласието на автора селектронното изявление;

-защитава съдържанието на електронното изявление от последващи промени;

Видно, използваният термин “обикновен” не е въведен легално от законодателя, но практиката е наложила това понятие с оглед отграничаването му от останалите видове електронни подписи, за която цел се използва и в настоящата работа.

Основен елемент на електронния подпис е конкретна информация (идентифициращо средство). Законът не въвежда ограничения по отношение на вида на информацията, Тя може да се състои от знаци, букви , символи, да бъде текстова, графична. За начинът на свързването и със електронното изявление обаче, страните трябва да се съобразят с въведения обективен критерии - осигуряване на достатъчно сигурност с оглед нуждите на оборота.(този критерии е относителен и се прилага отделно спрямо конкретни лица и конкретни правоотношения).

Като идентифициращо средство електронния подпис трябва да автентифицира електронното изявление – да носи информация за самоличността на автора и съгласието му с електронното изявление.

Изискването, че електронния подпис трябва да е свързан с електронното изявление по начин, защитаващ изявлението от последващи промени , предизвиква въпроси, свързани с неговото тълкуване.

Ако идентифициращото средство е известно и на двете страни – примерно , ако са договорили методът за шифроване на електронното изявление да бъде конвенционално шифроване на текста (един и същи код се използва за шифроване и разшифроване на текста), то тогава волеизявлението на отправителя не може да се счита гарантирано срещу евентуални промени в него , тъй като механизмът на създаване на електронния подпис не е под изключителния му контрол –той е съгласуван с адресата.

Изискваната от закона защита предполага използването на определени средства за идентификация (кодове, алгоритми) и изключва други, което в известна степен ограничава избора на страните и свободата на договаряне. В същия смисъл в чл. 14 е записано че “никой освен автора няма право на достъп до данните за създаване на електронен подпис” като в т.7 от “Допълнителните разпоредби” на закона е дадено оределение на “ Данни за създаване на подписа” – “уникална информация, като кодове или криптографски ключове, използвани от подписващото лице за създаване на подпис”.

Текстът на чл.14 ЗЕДЕП визира електронен подпис изобщо, което включва и обикновения електронен подпис, а както вече се отбеляза, логично , адресатът има достъп до електронния подпис, тъй като е съгласуван между него и автора . Освен това,

съгласно чл.13,ал.1т.1 страните могат да съгласуват “ всяка информация”, а не само “уникална информация като кодове или криптографски ключове”.

Тези вътрешно текстови противоречия биха могли да бъдат преодолени и въведеното изискване за защитеност на съдържанието на изявленията да се разглежда в контекста на прокламираните намерения на законодателя , за създаване на условия за насърчаване на правоотношенията , осъществявани по електронен път, чрез възприемане на ограничени правила и технологично- неутрална уредба на електронните подписи.

В този смисъл разгледаните текстове не могат да се тълкуват като ограничение спрямо използването на едно или друго средство за идентификация, а има характер на предписание страните да съгласуват автентификацията на изявленията си по начин защитаващ тяхното съдържание от несанкциониран достъп на трети лица.

За гарантиране на по- висока степен на защита на електронните изявления страните могат да използват ***Усъвършенстваният електронен подпис*** – чл.13,ал.1,т.2 ЗЕДЕП – преобразувано електронно изявление , включено , добавено или логически свързано със същото електронно изявление преди преобразуването.

Законът визира още ,че преобразуването ще се извършва чрез алгоритъм , включващ използването на частния ключ на асиметричната криптосистема. Алгоритмите, чрез които се създават данните за създаване на усъвършенстван електронен подпис (двойката криптографски ключове), както и алгоритмите , чрез които се създава самия подпис (хешираните съобщения , комбинациите между частен ключ и хеширано съобщение и псевдослучайни цифрови поредици) трябва да са признати за сигурни в практиката , да са възприети в действащи документи и международно признати спецификации. Изискванията за алгоритмите за усъвършенстван електронен подпис са определени с Наредба на МС (обн.,ДВ,бр.15 от 8 февруари 2002г.) .

Законодателят обръща изключително внимание на технологичната природа на подписа, което е видно от формулирането на определението, визиращо конкретен метод на създаване на подписа, така и от последващите текстове. Установени са изисквания по отношение механизма на създаване и проверка на подписа, като под механизъм за създаване на подписа се разбира – “ конфигуриран софтуер или хардуер, използван за въвеждане на данните за създаване на подписа”(т. 6 от Допълнителлните разпоредби на ЗЕДЕП). Данните за създаване на усъвършенстван електронен подпис всъщност представляват частният ключ, а данните за проверка – публичният ключ. Апаратните и програмни средства следва да осигурят надеждни механизми за създаване и проверка на алгоритмите, а не на самия подпис.

При традиционното собственоръчно подписване на документи, създаването на подписа и подписването на документа са идентични. При електронния подпис тези действия имат двояко значение. Създаването на подписа посредством алгоритми за генериране на частен и публичен ключ отразява технологичния характер на процеса, а подписването на електронния документ – характера на възникващите правни последици (документа се счита подписан в съответствие с изискванията на законодателството). Проверката на електронният подпис по смисъла на закона е всъщност проверка на частният ключ, посредством публичния ключ. От правна гледна точка проверката може да се определи като потвърждаване автентичноста на електронния подпис в електронния документ.

Алгоритъмът за създаване на подписа е под изключителния контрол на автора и никой освен него няма право на достъп до частния ключ(чл.18ЗЕДЕП). В случая по-прецизно би било да се използва термина “ титуляр на усъвършенстван електронен подпис”, вместо употребения “ автор”, тъй като “автора е лице , овластено да извършва

електронни изявления от името на титуляра на усъвършенствания електронен подпис" (чл.24,ал.1,т.3 ЗЕДЕП).

Гарантирането на връзката между публичния ключ и титуляра се осъществява от трета доверена страна , дефинирана легално в чл.19, ал.1 на закона като "доставчик на удостоверителни услуги" – лице, което издава удостоверения за усъвършенстван електронен подпис и води публичен регистър за тях (чл.28ЗЕДЕП). Изискванията по отношение дейността на доставчиците на удостоверителни услуги са детайлно уредени в ЗЕДЕП и Наредбата за дейността на доставчиците на удостоверителни услуги. Регулирането и контрола по предоставянето на удостоверителни услуги се извършва от Комисия по регулиране на съобщенията (КРС)

Основанието за възникване на правоотношенията между доставчик на удостоверителни услуги и бъдещ титуляр на усъвършенстван електронен подпис е сключването между тях на писмен договор (чл.23 ЗЕДЕП). Договорът ще бъде правно валиден и ако е съставен под формата на електронен документ.

Удостоверението за усъвършенстван електронен подпис е електронен документ, със съответни, изискуеми от закона реквизити (чл.24 ЗЕДЕП). То е електронна атестация, свързваща механизма на проверка на подписа с конкретно лице и удостоверява идентичността на това лице , т. е. връзката на титуляра с публичния ключ.

Законът урежда още процедурите по издаване, възобновяване, прекратяване действието на удостоверенията.

Ако по някакви причини удостоверението е невалидно – например, ако е с изтекъл срок или действието му е било прекратено, то документът няма автоматично да се девалидизира. В случай, че не противоречи на закона и обичайната практика той ще се счита подписан с обикновен електронен подпис, с правно валидни последици.

Тъй като ЗЕДЕП не посочва случаите, в които се използва усъвършенстван или обикновен електронен подпис и при положение, че в съответен специален закон това не е установено, страните могат да избират начина на автентифициране помежду си чрез споразумения , като отчитат характера на данните и търсената степен на защита предвид обичайната практика.

За разлика от създадената до известна степен свобода в частно правните отношения, в публичната сфера правна валидност е призната на ***Универсалния електронен подпис,*** с изключение когато МС е определил държавни органи, които могат да използват в отношенията помежду им друг вид електронен подпис.

В чл.33,ал.1 ЗЕДЕП , универсалният електронен подпис е определен като усъвършенстван електронен подпис, удостоверението относно който е издадено от регистриран доставчик на удостоверителни услуги. Изискванията за максимално висока сигурност предпоставят въвеждането на регистрационен режим на доставчиците. Регистрацията се извършва от Комисията по регулиране на съобщенията, която води регистър на удостоверенията за усъвършенстван електронен подпис на доставчиците. Редът за регистрацията е определен с Наредба за реда за регистрация на доставчиците на удостоверителни услуги.

Регистрираният доставчик на удостоверителни услуги може да удостоверява датата и часа на представяне на електронен документ, подписан с универсален електронен подпис.

Пълноценното използване в практиката на универсален електронен подпис ще бъде постигнато чрез постепенното създаване на необходимата инфраструктура и с приемане на съответните актове за това (Закон за приемането и издаването на електронни документи в съдебната система, вътрешни актове на държавни органи и органи на местно самоуправление и т. н.)

Въпреки изложените критики , че ЗЕДЕП неоправдано стеснява приложното поле на договорното регулиране в сферата на създаване и използване на електронните подписи, той е пълноценна нормативно – правно база , осигуряваща развитието на електронната търговия и изобщо на електронния документооборот в България.