Е-идентификация и е-удостоверителни услуги (Част I)

Какво е подпис в хартиения свят?

- Определение = саморъчно, т.е. ръкописно (и стилизирано) изписване на името и/или инициалите на издателя на документ

- Неръкописният подпис (например напечатан подпис) не представлява валиден подпис=> поместване на снимка на подписа; полагане на печат, изобразяващ подписа не са валидни саморъчни подписи

- Примери = подписване на договори, завещания, оферти, уведомления/предизвестия за прекратяване, искове, жалби и др. В някои случаи подписът може да доведе до допълнителни правни последици: „Всеки екземпляр на произведение на изобразителното изкуство, върху който стои саморъчно поставен подпис на автора, се счита за оригинал. Броят на оригиналите се определя от автора и се обявява по подходящ начин при първото разгласяване на произведението, като не подлежи на последващо изменение. Всеки екземпляр трябва да носи пореден номер.“

- Функция на саморъчния подпис

 Установяване на авторство – поради особения начин на изписване на саморъчния подпис чрез графологична експертиза при сравняване с други документи, съдържащи почерка на твърдения автор (т.нар. сравнителни образци), с голяма степен на вероятност може да се установи дали твърдяният автор на документа действително го е подписал или не. Експертизата изследва движението на ръката, наклона при писане, натиска с химикала и т.н.;

 Съгласие на автора с изявлението – след като авторът се е подписал под документа, той изразява съгласие с настъпването на

последиците, които документът материализира, в противен случай не би го подписал;

 Интегритет на изявлението – тази функция се свързва с факта, че авторът се подписва в края на документа, т.е. неговото съгласие с изявлението се простира до там, до където се е подписал. Всякакви текстови добавки, положени след саморъчния подпис, зачеркванията и др. под. с основание може да се оспорват като неистински, т.е. като неположени от самия автор. Ако авторът желае да нанесе някакви добавки или корекции, честа практика е след това авторът отново да положи подписа си като гаранция за истинността на добавката/корекцията;

 Стабилитет (неоттегляемост) на изявлението – с факта на подписването се създава правна сигурност, че авторът на изявлението не може своеволно да се откаже от него, респ. да оспорва последиците, които са материализирани в подписания документ.

- Използването на ИКТ предполага въпроса за регулирането на електронните подписи в цифрова среда

- Всяка възможност за електронно изявление от разстояние стана още по- важна по време на пандемията на COVID-19

- Правна рамка на е-подписите

 Регламент (ЕС) 910/2014 (eIDAS)

 Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ)

Видове е-подписи

Съществуват три различни вида е- подписи, като всеки следващ надгражда над предходния като изисквания, на които трябва да отговаря, а оттам и като степен на надеждност за гарантиране на авторството и интегритета на изявлението:

- Обикновен е-подпис (ОЕП)
- Усъвършенстван е-подпис (УЕП)
- Квалифициран е-подпис (КЕП)

ОЕП (1)

- ОЕП = данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, и които титулярят на електронния подпис използва, за да се подписва

Може да бъде всяка информация в електронна форма; технологично неутрален подход

 Определянето на автора може да става дори автоматично – напр. ако изявлението изхожда от специализирано приложение под контрола на автора (тъй като то се намира 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)

Примери

 Натискане на виртуални бутони в уебсайтове и мобилни приложения

 Отмятане на чекбоксове

 Натискане на линкове в имейли

+ пазене на лог файлове за това!

 Изпращане на SMS с кодове за потвърждение

 Дори полагане на саморъчен подпис върху хартиен документ, неговото сканиране (напр. в pdf формат) и изпращането на така сканирания е-документ от уговорен между страните имейл адрес

 Издадена от работодател електронна карта за достъп на служител, като „С всяко използване на картата ищцата [т.е. служителят] създава електронно изявление, чиято словесна част се генерира автоматично от системата за контрол и се изразява в посочване на датата и часа, в които е преодоляна защитата за достъп до сградата“

Примери

 Използване на електронна система за контрол на резултати от проверки на обекти, като резултатите се въвеждат от служителя с предоставен от работодателя таблет, и на система за GPS проследяване на автомобил, която автоматично генерира данни за позицията на автомобила, като според съда

 Размяна на кореспонденция по имейл, като във всяко електронно писмо се съдържат данни за неговия автор – две имена, длъжност и телефон за контакт на съответния служител на страните по договор за застраховка, а имейлите са „изпращани/получавани – от представители на двете дружества, на електронни адреси, регистрирани в мейл-сървърите им като потребители, като са видни са адресите от които, и до които, са процесните и-мейл, дата и час на получаване“

УЕП (1)

- УЕП = ОЕП, за който са изпълнени кумулативно още четири допълнителни изисквания

1. може да идентифицира титуляря на подписа – това означава, че чрез използването на УЕП трябва да се създаде увереност у адресата, че е-изявлението изхожда от конкретното лице, посочено като титуляр на подписа. Различни са техническите способи за постигане на това – идентифициране посредством потребителско име и уникална парола, въвеждани на ръка от клиента; идентифициране на служебната информация от токен устройства; използване на банкова карта (кредитна и дебитна) и пин код за теглене на пари от банкомат или за разплащания чрез ПОС терминал

2. свързан е по уникален начин с титуляря на подписа – това ще рече, за адресата да се създаде увереност, че е-изявлението изхожда само и единствено от лицето, посочено като титуляр на подписа, и че то не може да изхожда от друго трето лице. При горните примери това се постига посредством определени правила и процедури, въведени от банката, които предполагат установяване на самоличността на клиента посредством представяне на документ за самоличност и предоставяне точно на този клиент на уникалното потребителско име и парола/съответното токен устройство.

3. създаден е чрез данни за създаване на е-подпис, които титулярят на е-подписа може да използва с висока степен на доверие и единствено под свой контрол – при това изискване Регламентът подхожда технологично неутрално, т.е. не предписва конкретна технология, която да се използва. Важното е съответното средство да е единствено под контрола на титуляря. Контролът може да се осъществява както чрез физическо държане на средството (напр. банкова карта или токен, които се предоставят точно на определен клиент със задължение да не ги предоставя на трети лица), така и чрез обезпечаване на логически достъп до него (напр. чрез отдалечен

достъп посредством защитен профил до дадена система, където само титулярят може да активира функционалността за подписване);

4. свързан е с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях – чрез това изискване се обезпечава функцията интегритет, описана по-горе при саморъчния подпис. Логиката е използваната технология да гарантира сигурността на съдържанието на е-изявлението, като позволява установяването на всякакви последващи промени в него. Необходимо е съответната технология да гарантира определено ниво на сигурност, което страните да приемат за достатъчно в отношенията си, но не и гарантиране на най-високото ниво на сигурност, което – видно от изложеното по-долу – се постига при третия вид е-подпис, а именно квалифицирания е-подпис. Примери за това са криптиране на връзката посредством симетрични ключове, генерирани от токен устройство; използване на специализирани приложения за електронно банкиране; при вече идентифициран автор посредством потребителско име и/или парола – изграждане на свързаност посредством 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

КЕП (1)

• КЕП = УЕП, за който са изпълнени кумулативно още две допълнителни изисквания

1. той е създаден от устройство за създаване на КЕП, и

2. основава се на квалифицирано удостоверение за електронни подписи

- N.B.!!! При КЕП е налице нормативноустановена технология, която да се използва – инфраструктурата на публичния ключ
- Двойка ключове – частен и публичен

 Те представляват двойка числа, които не са еднакви, но са математически относими при прилагането на алгоритъм за асиметрично криптиране. Тези числа са уникални, т.е. на даден частен ключ отговаря само един публичен ключ, а от публичния ключ е невъзможно извеждането на стойността на частния ключ

 Частният ключ следва да е известен единствено на титуляря на подписа и се използва за създаването на е-подписа

 Публичният ключ може да се разкрива на трети лица, за да проверяват авторството и интегритета на е-изявлението

 Връзката между частния и публичния ключ се удостоверява посредством удостоверение за е-подпис – това е специален документ, който се издава от трето лице – доставчик на удостоверителни услуги – съдържащ името на автора на изявлението; неговия публичен ключ, съответстващ на държания от него частен ключ; както и други, изчерпателно изброени реквизити

 Чрез него у адресатите се създава сигурност, че публичният ключ, посочен в удостоверението, действително е притежание на автора на подписа. Доставчиците на удостоверителните услуги поддържат публичен регистър, където се публикуват удостоверенията за КЕП и където всяко трето лице може да провери верността на публичните ключове на доставчиците.

 При издаването на удостоверение доставчикът на удостоверителни услуги следва да: (1) е установил самоличността на автора на е-подписа (напр. чрез представяне на документ за

самоличност при явяване в офис или чрез проверка на документ за самоличност от разстояние, доколкото някои доставчици предлагат услугата издаване на КЕП от разстояние); (2) се е уверил, че (а) частният ключ е в държане на автора и (б) че представеният публичен ключ съответства на държания от автора частен ключ.

- Устройствата за създаване на КЕП представляват софтуер или хардуер, които се използват за въвеждане на данните за създаване на е-подписа (напр. токени, карти и др.).

- Конкретните изисквания, на които тези устройства трябва да отговарят, са уредени в Приложение II към Регламент 910/2014 – напр.:

Устройствата за създаване на квалифициран електронен подпис гарантират чрез подходящи технически и процедурни средства най-малко, че:

- поверителността на данните за създаване на електронен подпис, използвани за създаването на електронния подпис, е разумно гарантирана;

- данните за създаване на електронен подпис, използвани за създаването на електронния подпис, на практика се срещат само веднъж;

- данните за създаване на електронен подпис, използвани за създаването на електронния подпис, са обезпечени в достатъчна степен и не могат да бъдат извлечени, а електронният подпис е надеждно защитен срещу подправяне чрез използване на наличната към момента технология;

- данните за създаване на електронен подпис, използвани за създаването на електронния подпис, могат да бъдат надеждно

защитени от законния титуляр на електронния подпис срещу използване от други лица.

- Липсата на такова устройство в процеса по създаване на КЕП „девалидира електронния подпис като квалифициран“
- Извличане от всеки документ чрез хеш алгоритми на уникално число (контролно число), което показва дали са направени промени в него (дори един BIT води до различно контролно число)
- Контролното число се криптира чрез частния ключ. За всеки документ електронният подпис е различен, дори ако е направен от един и същ частен ключ
- След „подписване“ на електронното изявление, приложен към него се прилага криптираното контролно число
- Автоматична проверка чрез публичния ключ:

1) За контролното число. Адресатът декрптира контролното число в момента на „подписване“, извлича ново контролно число от полученото изявление и ги сравнява, и

2) За авторство, т.е. дали електронният подпис е създаден чрез съответния частен ключ.

N.B.!!! КЕП дава най-голяма сигурност с оглед установяване на авторството и интегритета на е- изявлението

Правна сила на видовете е-подписи

С настоящия регламент следва да се установи принципът, че правната сила на електронен подпис не може да бъде оспорена на основанието, че той е в електронна форма или че не отговоря на изискванията за квалифицирания електронен подпис. Правната сила на електронните подписи обаче се определя от националното право,

с изключение на включените в настоящия регламент изисквания квалифицираният електронен подпис да има същата правна сила като саморъчния подпис.

- N.B.!!! ОЕП & УЕП = саморъчни подписи, когато това е уговорено между страните

  Изрична клауза в договор

  Чрез конклудентни действия – напр. поради факта на обменяне на е-изявления чрез определена технология (е-поща, SMS, социална мрежа, чат програми и мобилни приложения (Skype, Viber, WhatsApp, Telegram, Signal, WeChat, Facebook Messenger и много други) и т.н.) и надлежното изпълнение на възникналите по силата на така обмените е-изявления задължения . Това се обяснява по следния начин: Авторът, отправяйки изявление към другата страна, очевидно го прави с ясното съзнание, че иска да бъде идентифициран като автор. Адресатът от своя страна има право на преценка да приеме или не дали изявлението изхожда от автора и ако му отговори или съобрази поведението си с изявлението, очевидно приема, че изявлението изхожда от твърдения автор

- N.B.!!! КЕП = саморъчен подпис по силата на закона. КЕП, основан на квалифицирано удостоверение, издадено в една държава членка, се признава за квалифициран електронен подпис във всички други държави членки.

Доставчици на удостоверителни услуги (1)

- Доставчици на удостоверителни услуги (ДУУ) = физическо или юридическо лице, което предоставя една или повече удостоверителни услуги като доставчик на квалифицирани или на неквалифицирани удостоверителни услуги

• Доставчик на квалифицирани удостоверителни услуги (ДКУУ) = доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от надзорен орган

• Изисквания за сигурност

 Предприемат подходящи технически и организационни мерки за управление на рисковете за сигурността на предоставяните от тях удостоверителни услуги; подход, основан на риска; предотвратяване и свеждане до минимум на въздействието на инциденти, свързани със сигурността, и за информиране на заинтересованите страни относно нежеланите последици от такива инциденти

 Задължения за уведомяване

 В случай на пробив в сигурността или нарушаване на целостта, които имат съществено въздействие върху предоставяната удостоверителна услуга или върху съхраняваните лични данни, ДКУУ и ДУУ уведомяват за това без излишно забавяне, но при всички случаи в срок от 24 часа от момента, в който са узнали за настъпилото събитие, надзорния орган и, когато е приложимо, други компетентни органи, например компетентния национален орган в областта на информационната сигурност или органа по защита на данните.

 Когато има вероятност пробивът в сигурността или нарушаването на целостта да окажат негативно въздействие върху физическо или юридическо лице, на което е предоставена удостоверителната услуга, ДУУ уведомява без излишно забавяне за пробива в сигурността или нарушаването на целостта и въпросното физическо или юридическо лице.

 При необходимост, и особено ако пробивът в сигурността или нарушаването на целостта засягат две или повече държави членки, уведоменият надзорен орган информира надзорните органи в останалите засегнати държави членки и ENISA. Ако прецени, че разгласяването на пробива в сигурността или нарушаването на целостта е в обществен интерес, уведоменият надзорен орган информира обществеността или изисква от ДУУ да направи това.

• Веднъж годишно надзорният орган представя на ENISA обобщение на уведомленията за пробиви в сигурността и нарушения на целостта, получени от ДУУ.

• ДКУУ са обект на одит (за тяхна сметка) най-малко веднъж на 24 месеца от орган за оценяване на съответствието; ДКУУ представят на надзорния орган съответния доклад за оценяване на съответствието в срок от три работни дни след като го получат.

 Надзорният орган може по всяко време да извърши одит или да поиска от орган за оценяване на съответствието да направи оценяване на съответствието на ДКУУ за тяхна собствена сметка

 Непредприемане на мерки за изпълнение на неизпълнени от ДКИИ изисквания може да доведе до отнемане на квалифицирания статут на ДКУУ или на съответната предоставяна от него услуга

• Процедура по стартиране на КУУ – уведомление до надзорния орган за намерението си заедно с доклад за оценяване на съответствието, съставен от органа за оценяване на съответствието; вписване в Доверителни списъци

• Други изисквания за ДКУУ

 Да проверява чрез подходящи средства и в съответствие с националното право самоличността и, ако е приложимо, всички

специфични данни за физическото или юридическото лице, на което се издава квалифицираното удостоверение

 Да информира надзорния орган относно всяка промяна в предоставянето от него на квалифицирани удостоверителни услуги, включително за намерението да преустанови тези дейностти

 Да наема персонал и, ако е приложимо, подизпълнители, които притежават необходимите експертни знания, надеждност, опит и квалификация и са преминали подходящо обучение относно правилата за сигурност и защита на личните данни, и прилага съответстващи на европейските или международните стандарти административни и управленски процедури

 Да поддържа достатъчни финансови ресурси и/или сключва подходяща застраховка за отговорност в съответствие с националното право, за да покрива евентуални искове за вреди

 Да използва надеждни системи и продукти, които са защитени срещу промяна, и гарантира техническата сигурност и надеждност на поддържаните от тях процеси

 Да взема подходящи мерки срещу подправяне и кражба на данни

 Да записва и съхранява на разположение за подходящ срок, включително след като доставчикът на квалифицирани удостоверителни услуги е преустановил дейността си, цялата имаща отношение информация във връзка с данните, издадени и получени от доставчик на квалифицирани удостоверителни услуги, и по-специално с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата. Тези записи могат да бъдат направени по електронен път;)

- Да осигурява законосъобразна обработка на лични данни
- Ако реши да отмени удостоверение, да регистрира тази отмяна в неговата база данни с удостоверения и да публикува отменения статут на удостоверението своевременно, но във всички случаи в срок до24 часа след като бъде получено искането
- …. (вж. чл. 24 от Регламента)

- Отношенията с титуляря се уреждат с договор (чл. 23 ЗЕДЕУУ)
- Надзорен орган за България - Комисия за регулиране на съобщенията, уебсайт (https://crc.bg/); вж също:

Изводи

- Правото е създало правен режим за подписване на документи във виртуална среда
- Е-подписите могат да са равносилни на саморъчния подпис

в хартиения свят

- Е-подписите имат определени особеност (напр. за ОЕП/УЕП е необходимо съгласие, за да бъдат приравнени на саморъчния подпис, докато КЕП е приравнен по силата на закона)
- КЕП от една държава членка се признава в целия ЕС; осигурява се от 3-то лице - ДУУ
- Е-подписите имат множество приложения – в е-търговията,

е-управлението, защитата на личните данни и пр.