РЕЖИМ И ПРАКТИЧЕСКО ПРИЛОЖЕНИЕ НА ЕЛЕКТРОННИТЕ ПОДПИСИ - УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС

Автор:

Адв. Георги Димитров
Адв. дружество Димитров, Петров и Ко.
Хон. преподавател в СУ "Св. Климент Охридски"
Ел.поща: george.dimitrov@dpc.bg

Така, както обикновения електронен подпис[1], усъвършенстваният подпис е средство за автентификация. За разлика от обикновения подпис, обаче, използването на усъвършенствания предполага много по-голяма сигурност в електронния оборот при установяване на автора на електронното изявление и липсата на изменение в съдържанието му от изпращането до получаването му.

Принцип на действие

Усъвършенстваният електронен подпис по смисъла на ЗЕДЕП е дефиниран като преобразувано електронно изявление, включено, добавено или логически свързано със същото електронно изявление, преди преобразуването. Преобразуването трябва да се осъществява чрез алгоритми, включващи използването на частният ключ на асиметрична криптосистема.

Какво означава това?

Принципът на използването и действието на електронните подписи се базира на 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 частния ключ със най-съвременните информационни и технологични средства.

Създаването на ключовете по своята същност представлява генериране посредством съответни математически алгоритми на асиметрична криптография и предоставянето на частния ключ на титуляра, респ. на упълномощения от титуляра автор[2]. 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. В задължение 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.

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 (чл.14 от ЗЕДЕП). Той се

---

[1] Вж. Димитров, Г., Режим и практическо приложение на електронните подписи – Обикновен подпис, сп. Пазар и право, кн.1, 2003 г.

[2] За повече подробности виж ITU-T Recommendation X.509; също Electronic Signatures – Survey of the Law and Practice in the European Union, ICIT, 1998, Woodhead Publishing Limited, стр.58; Introduction to cryptography, 1990-1999 Network Associates, Inc.

използува за "подписване" на електронното съобщение. Ако частният ключ стане достояние на друго лице, то същото ще може да подписва изявления от името на титуляра и да ангажира неограничено неговата правна сфера. Интересите на титуляра, респективно на обществото сериозно биха се застрашили.

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.

Използуването на един ключ за осъществяване на шифриране (криптиране) и различен ключ за дешифриране (декриптиране) е възможен благодарение на създадените алгоритмични методи на асиметрична криптография[3].

"Подписването" на електронния документ с усъвършенстван електронен подпис се базира на извличането от даден електронен документ посредством определени алгоритми (хеш-алгоритми) на уникално математическо извлечение на този документ, наричано "хеш идентификатор" или "електронно резюме". Характерно е, че извлеченото "електронно резюме" отговаря само на документа, от който е извлечено. С криптирането на "резюмето" с частния ключ се създава самият електронен подпис. С други думи усъвършенстваният електронен подпис е криптирано с частния ключ електронно резюме 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. За това 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. Самият закон е също непоследователен в тази насока (вж. чл.22, т.8, чл.28 ал.1, чл.33, ал.2, т.1 и др.). Често законодателят използува термина "притежава електронен подпис", като в зависимост от контекста и систематичното място на термина визира именно притежаване на частен ключ или съответно на публичен ключ.

Практически след създаването на електронния подпис ("подписването"), към електронното изявление се добавя преобразуваното с частния ключ "електронно резюме" (електронният подпис) и така добавеното и логически свързано съобщение в пакет се изпраща на адресата.

От така изложеното вече лесно може да се разбере смисъла на нормата на чл.16, че усъвършенстваният електронен подпис е преобразувано с частен ключ посредством алгоритми на асиметрична криптография електронно изявление, включено, добавено или логически свързано със същото електронно изявление, преди преобразуването.

В електронния документооборот от изключителна важност е да съществува сигурност, че изпращаните електронни изявления 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 осъществяване на проверка на подписа от адресата на подписаното електронно изявление.

---

[3] За разлика от методите на симетричната криптография, където с един и същ ключ се криптира и декриптира.

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 обратен процес на този на подписването. Осъществява се чрез публичния ключ, който е направен достояние на адресатите. Първо адресатът декодира електронния подпис и получава "електронното резюме", такова, каквото е било към момента на създаване на подписа. След това се извлича ново резюме от електронното изявление и новополученото резюме се сравнява с декодираното. 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 електронно резюме ще се различава от декодираното. Така лесно може да се установи нарушаване на интегритета на изявлението.

Подписването и проверката на електронния документ стават автоматично посредством специализиран софтуер (напр. при подписване на електронна поща стандартизираните популярните софтуерни приложения като Eudora, Microsoft Outlook, Outlook Express и т.н. поддържат такава функционалност).

Удостоверение за публичния ключ

Както бе отбелязано, усъвършенстваният 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 титуляра или 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 титуляр или 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 титулярът 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.

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 усъвършенстван електронен подпис[4]. Третата доверена

[4] Според Директивата и в чуждестранната литература - "digital certificate". В българската литература се използват като равнозначни термини "цифров сертификат", "електронен сертификат" или "сертификат за електронен подпис".

страна е дефинирана легално в нашия закон като "доставчик на удостоверителни услуги"[5] (ДУУ).

Удостоверението за електронен подпис е специален електронен документ, съдържащо името на титуляра и неговия публичен ключ и други предписани от закона реквизити. Това удостоверение се подписва с усъвършенстваният 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 визиран в издаденото удостоверение, е действително притежание на титуляра на подписа. По този начин всички трети лица – адресати на електронни съобщения, подписани с усъвършенстваният електронен подпис на титуляра, ще могат да установят дали изпратеното съобщение изхожда точно от титуляра, тоест дали съобщението е автентично. Следователно, за да се издаде удостоверение е необходимо доставчикът на удостоверителни услуги да се убеди и провери самоличността на титуляра и фактите, че частният ключ се държи от него и че представеният публичен ключ, съответства именно на държаният от титуляра 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 достъпен списък в електронния регистър на удостоверенията, поддържан от доставчика.

Ако електронният подпис, положен върху електронното изявление е придружен от валидно електронно удостоверение, издадено от доставчик на удостоверителни услуги, то същият ще се счита за усъвършенстван, а когато е издадено от регистриран доставчик - за универсален. С други думи, от гледна точка на правото наличието на валидно придружаващо удостоверение е предпоставка усъвършенстваният, респ. универсалният електронен подпис да се квалифицират като такива.

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

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 автоматизирано от специализираните софтуери, поддържащи функционалност за подписване и проверка на подписани съобщения.

Правна същност и последици

Понятието "усъвършенстван електронен подпис" не се покрива смислово с това на Директивата. Практически там смисълът на понятието "усъвършенстван електронен подпис" се съотнася с този на "обикновен електронен подпис" според нашия закон. Освен това, за разлика от ЗЕДЕП, Директивата на предвижда изискване за

[5] "Certification Service Provider"

усъвършенстваният електронен подпис да има издадено удостоверение от доставчик на удостоверителни услуги.

Смисълът на понятието според нашия закон се покрива със този, който се възвежда от чл.5, ал.1 на Директивата – т.нар. "квалифициран електронен подпис". Според цитираният член това е този усъвършенстван електронен подпис, за който е издадено квалифицирано удостоверение и е създаден посредством сигурен механизъм за създаване на подписа.

Така както обикновения подпис, усъвършенстваният електронен подпис има значението на саморъчен (чл13, ал.2). Това правило не се прилага за случаите, когато адресат или титуляр на подписаното електронно изявление е държавен орган или орган на местното самоуправление. Но и в тези случаи е възможно усъвършенстваният подпис да има последиците на саморъчен. Министерски съвет е овластен от ЗЕДЕП да определи държавните органи, които могат да използуват в разменяните електронни изявления между тях усъвършенстван или обикновен електронен подпис.

Значението на приравняването на правните последици на усъвършенстваният подпис със саморъчния се проявява от материално-правна гледна точка, но не и от процесуално-правна. Това означава, че доколкото страните в един граждански процес представят като доказателствено средство за доказване на наличието или липсата на определени факти електронен документ, подписан с усъвършенстван електронен подпис, съдът следва да зачете същата правна стойност, каквато би зачел на подписания писмен документ. Това е така, защото законът изрично възвежда фикция по отношение на материално-правните последици от използуването на усъвършенстваният подпис. При условие, че в правоотношенията помежду им отправянето на изявления посредством подписан с усъвършенстван подпис електронен документ има значението на отправяне с подписан със саморъчен подпис писмен документ (арг. от чл.13, ал.2 във връзка с чл.3, ал.2), то ще произтекат същите материално-правни последици, както от използуването на подписан писмен документ. Следователно, на страните не може да бъде отказана възможността да докажат в рамките на процеса определени факти, с представянето на подписан с усъвършенстван подпис електронен документ. Представянето на самия електронен документ може да стане във възпроизведен вид или в електронен вид чрез съответния носител. Точността на възпроизвеждането на електронния документ и валидността на електронния подпис може да се установи с експертиза.

Не би могло, обаче, страните да използуват електронния подпис в упражняването на процесуалните си права и изпълнение на процесуалните си задължения. Приемането и издаването на електронни документи в съдебната система (напр. издаване в електронна форма на съдебни решения, подаване на искови молба и т.н.) следва да се уреди със закон.

Универсален електронен подпис

Нашият закон възвежда като особен вид усъвършенстван електронен подпис *универсалния електронен подпис*. Разликата между него и усъвършенстваният подпис се състои единствено в това, че удостоверението за него се издава от регистриран доставчик на удостоверителни услуги.

Универсалният електронен подпис има значението на саморъчен по отношение на всички, включително на всички държавни органи и органите на местното самоуправление.

Ex lege универсални са подписите на всички регистрирани доставчици, на Комисията за регулиране на съобщенията, с които тя подписва актовете, които издава по силата на закона (чл.33). Изискване на използуване на универсални подписи има и по отношение на съдебната система, макар използуването да следва да се уреди със специален закон, както и по отношение на държавните органи, които не са на подчинение на МС (напр. Конституционния съд, Сметната палата, Българска народна банка и т.н.).