ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

ПРОБЛЕМИ ПРИ ДЪЛГОСРОЧНОТО СЪХРАНЕНИЕ НА ЕЛЕКТРОННИ ДОКУМЕНТИ, ПОДПИСАНИ С КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ

Александър Кирков
Университет по библиотекознание и информационни технологии

Димо Водкаджиев
Окръжен съд – Добрич

Резюме: *Електронните документи са основна и неразделна част от днешния дигитален свят. Бурното използване на електронни документи в последните години се дължи на икономията на време и средства в сравнение с книжните. Електронно подписани документи се ползват в много държави, като тяхната правна стойност и надеждност се осигуряват именно от електронните подписи. Квалифицираните електронни подписи (QES) предоставят най-високото ниво на правна сигурност и са еквивалентни на собственоръчния подпис. Квалифицираният електронен подпис се създава въз основа на цифрово удостоверение, което обаче се издава за определен срок и след този срок, за да запазят своята правна сила и надеждност, квалифицираните електронни подписи трябва да бъдат поддържани чрез специализирани технологии и процеси за дългосрочно съхранение. Невъзможността да се провери квалифицираният електронен подпис след изтичането на срока на удостоверението, както и други негови атрибути създават множество пречки в използването на електронните документи. Тази статия има за цел да акцентира върху проблемите, свързани с дългосрочното съхраняване на електронните документи, подписани с квалифициран електронен подпис, и разглежда в технически аспект възможностите и нивата на електронните подписи спрямо приетите в ЕС нормативни документи.*

Ключови думи: *електронен подпис, КЕП, съхранение на КЕП, времеви печат, валидност на КЕП, електронен документ*

ВЪВЕДЕНИЕ

Бурното използване на електронни документи в последните години се дължи на икономията на време и средства в сравнение с книжните. Електронно подписани документи се ползват в много държави, като тяхната правна стойност и надеждност се осигуряват именно от електронните подписи.

През 2014 г. Европейският парламент и Съветът на Европа публикуваха Регламент (ЕС) № 910/2014, с който унифицираха изискванията към електронните подписи в ЕС, и това беше важна стъпка в плановете за дигитализация на Европейския съюз. Именно този регламент издига електронния документ на нивото на хартиения, като не само приравнява квалифицирания електронен подпис на саморъчния, но и включва правилото, че един документ не може да бъде отказан или оставен без разглеждане само за това, че е електронен.

Използваните за създаване на квалифицирани електронни подписи удостоверения се издават за ограничено време и често то е със срок от една година. След изтичане на този срок при проверка на подписа е видно, че проверяваният КЕП е базиран на невалидно удостоверение (сертификат). Оттук се появява и дилемата дали след като техническо удостоверението за създаване на КЕП не е валидно, е валиден подписът, създаден чрез това удостоверение?

Необходимост от дългосрочно съхранение на електронни документи, подписани с

квалифицирани електронни подписи, има в много и различни сфери, като при дългосрочното съхраняване на електронно подписани документи задължително трябва да се запази статусът на валидност на положения подпис.

Доказателствената сила на документите във времето зависи от възможността да бъде безспорно удостоверена валидността на положените подписи под тях. При масовата електронизация във всички нива на администрацията и бизнеса и приравняването на квалифицирания електронен подпис към ръчно положения и в националното законодателство ежедневно се създават хиляди електронни документи, подписани с квалифицирани електронни подписи, които трябва да бъдат съхранявани в продължение на много години поради различни нормативни изисквания. Ярък пример са съдебните актове по граждански дела с предмет искове по семейния кодекс или фирмените дела по ЗЮЛНЦ, които трябва да се съхраняват в продължение на над 100 години.

Разбира се, в т. 61 от преамбюла на Регламент (ЕС) № 910/2014 на ЕП и Съвета е посочен следният текст: „Настоящият регламент следва да осигури дългосрочното съхраняване на информация, за да се осигури правната валидност на електронните подписи и електронните печати за продължителен период от време и да се гарантира, че те могат да бъдат валидирани независимо от бъдещи промени в технологиите“, и технически това може да бъде реализирано чрез т.нар. нива на подписване.

Нивата на подписване не зависят от формата на подписване (XAdES, CAdES, PAdES) и се обозначават с латински букви след него. Например: Ако подписваме файл в pdf формат с най-ниското ниво на подписване, то индикацията на нивото на подписване би трябвало да е Pades–B или Pades_B. В този материал ще се спрем само на видовете подписване BASELINE, които се ползват най-масово в България.

BASELINE НИВА НА ПОДПИСВАНЕ, ПРИЛОЖИМИ КЪМ ФОРМАТИТЕ НА КВАЛИФИЦИРАНОТО ЕЛЕКТРОННО ПОДПИСВАНЕ

Към всеки от регламентираните формати на квалифицираното електронно подписване (CAdES, PAdES и XAdES) могат да бъдат приложени четири различни нива на подписване – BASELINE_B, BASELINE_T, BASELINE_LT и BASELINE_LTA, като всяко ниво се различава по информацията, която се съхранява в подписа (различни атрибути), и се показва с латински букви след формата на подписване. Форматите и нивата на подписване са описани подробно в техническите спецификации:

– Technical Specification CMS Advanced Electronic Sigantures (CAdES) – ETSI TS 101 733;

– Technical Specification PDF Advanced Electronic Sigantures (PAdES) – ETSI TS 103 172;

– Technical Specification XML Advanced Electronic Sigantures (XAdES) – ETSI TS 103 171, които са част от стандарта ETSI EN 319 102 и Регламента.

Важно е да отбележим, че различните формати на подписване са предназначени за подписване на различни формати на данни (файлове) и не се различават по отношение на сигурността на подписване, докато нивото на подписване е пряко свързано с информацията (атрибутите), която се съхранява за електронния документ и електронния подпис, което е от съществено значение за правната сила на конкретния документ.

Ниво на електронно подписване BASELINE_B

Нивото на подписване BASELINE_B представлява най-ниското ниво на съдържание на информация по отношение на подписания документ в рамката на ETSI стандартите и се нарича базово ниво на електронния подпис.

BASELINE_B осигурява цялост на подписания документ и неотменимост на положения електронен подпис, като включва информацията за оригиналния документ, атрибутите на удостоверението за създаване на квалифициран електронен подпис и самия подпис във вид на цифров криптографски сертификат.

BASELINE_B като ниво на подписване не позволява на подписаните документи да се ползват с висока степен на доверие поради липсата на сигурна информация за време на подписване и

невъзможността да бъде проверен автоматизирано подписът след изтичане на срока на валидност на удостоверението, както и други атрибути. Като едно от малкото предимства на BASELINE_B нивото пред по-високи нива на подписване може да се изтъкне възможността за лесно и евтино внедряване и имплементация в съществуващи информационни системи.

Ниво на електронно подписване BASELINE_T

BASELINE_T е второто от нивата на електронно подписване, определено от ETSI стандартите. То представлява надграждане над базовото ниво BASELINE_B чрез добавянето на удостоверение за време (TimeStamp) или наричано още „времеви печат“, което като атрибут на подписа носи информация за подписването на документа към определена дата и час. С добавянето на времеви печат се добавя допълнителен елемент на сигурност и доверие над базовото ниво.

Времевият печат или още удостоверението за време (TimeStamp) е атрибут на КЕП, който удостоверява времето на подписване и съдържанието на електронен документ към този момент. Този атрибут може да се използва за отчитане на извършена работа към даден момент, за доказване на авторство към определена дата и други. Записът на времето за подписване е криптографски защитено и на практика е невъзможно да бъде манипулирано. В случаите, когато времето на подписване е взето от часовника на локалния компютър или от локален сървър, то това се счита за голям недостатък на електронния подпис поради това, че локалният компютър или сървър са изцяло под контрола на подписващия и времето на подписване не може да се удостовери с висока степен на доверие и сигурност. В случаите, когато времето на подписване е получено от независим сървър на време, то тогава може да бъде прието, че времето на подписа е реално и прецизно.

Тук, разбира се, е мястото да спомена, че съществува и квалифициран електронен времеви печат, който допълнително може да удостовери времето на подписване на документа или на различни редакции на един и същ документ по хронология. По същество квалифицираният електронен времеви печат утвърждава, че електронният подпис е създаден преди момента, указан в него.

Нивото BASELINE_T е подходящо за използване в случаите, когато имаме документи, които изискват доказано време на подписване. Внедреното удостоверение за време в BASELINE_T предотвратява възможността за промяна на точния момент на подписване или така наречената антидатиране.

Добавянето на удостоверение за време неизменно увеличава сложността на процеса на подписване и изисква допълнителни ресурси, като същевременно се повишават и разходите. Също така е важно да се отбележи, че само ползването на независими и прецизни сървъри на точно време се ползват с висока степен на доверие, а не само техническото добавяне на този атрибут към електронния подпис.

Ниво на електронно подписване BASELINE_LT

Нивото BASELINE_LT (известно още като BASELINE LONG TERM) е третото от нивата на електронно подписване, разработени от ETSI, надграждайки предшестващото ниво BASELINE_T и съответно съдържа всички атрибути на BASELINE_T, към които са добавени допълнителна информация (атрибути), като VRI (Verification Related Information) данни към DSS (Document Security Store), както и данни за анулиране, като OCSP (Online Certificate Status Protocol) отговори или CRL (Certificate Revocation List) и веригата на сертификати, от потребителския сертификат до Root CA сертификат. Това прави възможно валидирането на подписания документ чрез съдържанието на самия файл.

– Verification Related Information (VRI) представлява набор от данни, включващи имена, електронни пощи, номера и много други, които се използват за удостоверяване на самоличността на подписващия. Основната цел на VRI е да предоставя необходимата информация за извършване на проверки за истинността на подписания документ, както и дали има промени след подписването.

– Document Security Store (DSS) е основен и много важен компонент в необходимата инфраструктура за създаване и проверка на електронните подписи, тъй като осигурява необходимите

механизми за управление на сигурността и автентичността на подписаните документи. DSS играе ключова роля в осигуряването на автентичността, целостта и недостъпността на подписаните документи. Функции на Document Security Store са осигуряване на сигурно защитено хранилище на електронно подписани документи, управление на цифровите сертификати и криптографски ключове, осигуряване на сигурен механизъм за електронно валидиране на електронни подписи, запазване на конфиденциалността на съхраняваните документи чрез контрол на достъпа, проследяване и одитиране на всички действия, свързани с електронно подписани документи, осигуряване на дългосрочно съхранение на електронно подписани документи, като се гарантира тяхната наличност и неизменност през целия период на съхранение. DSS съдържа информация, свързана с валидирането, само за подписи на документи, представени във формат PKCS#7 (и негови производни).

– Online Certificate Status Protocol (OCSP) е комуникационен протокол, който се използва за проверка на валидността на цифрови сертификати в реално време. OCSP е важен компонент в инфраструктурата на издаване на удостоверението за квалифициран електронен подпис, който от своя страна е базиран на цифров сертификат. Основната цел на OCSP е да предоставя текуща информация за статуса на цифровите сертификати, като позволява на клиентите да проверят дали даден сертификат е валиден, анулиран или изтекъл.

– Certificate Revocation List (CRL) представлява списък на анулирани сертификати, който е публично достъпен. Тези списъци се създават и поддържат от издателите на удостоверенията за квалифицирани електронни подписи (цифровите сертификати). Този списък съдържа сертификати, които са анулирани предсрочно и вече не са валидни, като за анулираните сертификати се записва в него следната конкретна информация: серийните номера на всички анулирани сертификати; точна дата и час на анулиране на всеки сертификат; като опция в списъка може да е налична и информация относно причината за анулиране на конкретен сертификат. Този списък е от особена важност, тъй като предпазва от злоупотреби като подписване с анулиран електронен подпис.

– Root CA сертификат е основополагащ елемент в инфраструктурата на публични ключове, който се използва за удостоверяване на самите издатели на сертификати, които са част от удостоверенията за квалифициран електронен подпис. Този сертификат служи за еталон и чрез него могат да бъдат проверявани всички издадени сертификати (удостоверения за КЕП) относно тяхната автентичност и надеждност.

Накратко казано, BASELINE_LT – надгражда базовото ниво на подпис с удостоверено време (BASELINE_T), като към неговите атрибути са добавени допълнителни, осигуряващи възможността да се провери валидността на подписа единствено въз основа на подписания файл, без да се изискват допълнителни проверки като статус на удостоверението за КЕП или търсене на сертификационната верига на удостоверението за КЕП в регистрите на издателя. Също така това ниво осигурява информация за валидността на подписа при дългосрочно съхранение на подписания файл.

Разбира се, с всяко надграждане на нивото на подписване се увеличава и сложността, респективно и разходите за неговото софтуерно реализиране. В случая усложняването и повишаването на разходите са обусловени от самите процедури за архивиране и управление на криптографските данни и от нужните ресурси за това.

Ниво на електронно подписване BASELINE_LTA

BASELINE_LTA (BASELINE LONG TERM WITH ARCHIVE) е най-високото ниво на електронно подписване според Европейските стандарти (ETSI). Това ниво осигурява дългосрочната валидност при проверка на електронните подписи и на подписаните документи чрез архивиране и защита на криптографските материали за продължителен период от време. Нивото BASELINE_LTA съдържа всички атрибути на BASELINE LONG TERM, като към тях се добавят и допълнителни архивни печати (Archive Timestamps) на определени интервали, за да се обнови доказателствената стойност на електронния подпис, и позволява периодично актуализиране на удостовереното време и валидацията на подписа дълго време след създаването му.

ЗАКЛЮЧЕНИЕ

Поради това, че електронните документи могат да се създават и изпращат по електронен път и това спестява много сили и средства, те са все по-предпочитани. Електронният документооборот нараства ежедневно и начинът на електронно подписване е от значение за валидността и правната стойност на документите.

От друга страна, материята на електронния подпис е специфична и свързана с цифрови технологии, което от своя страна я прави трудна за хора без технически познания и правна грамотност.

През последните години станахме свидетели на това как електронно подписани документи стават невалидни след изтичане на удостоверението на подписалия ги поради това, че е използвано ниско ниво на подписване. Такива случаи бяха масови и доведоха до завеждането на съдебни дела и необходимостта от технически експертизи на подписаните документи по тези дела.

Също така е имало опити за подписване на документ с предварително анулирано удостоверение, което пак поради използване на ниско ниво на подписване е видно едва след проверка валидността на документа.

Така поради липсата на знания за техническите възможности за съхранение и проверка на квалифицираните електронни подписи беше компрометирана основната идея на Регламент (ЕС) № 910/2014 на ЕП и Съвета, а именно да се създаде система за издаване и получаване на електронни документи с висока степен на доверие и сигурност.

На практика досега най-често ползваните нива на квалифицирано подписване на електронни документи са BASELINE_B и BASELINE_T, от които първият не носи информация за точното време на подписване, а и двата не съхраняват статуса на валидност на подписа след изтичане на удостоверението, който най-често е една година. Разбира се, в случаите при подписване на електронна кореспонденция и документи, които нямат висока правна стойност и/или не изискват дългосрочно съхранение, това е приемливо, но за документи, издадени от държавната или общинска администрация, тези нива на подписване са неприемливи и създават редица трудности.

В технически аспект нивата на квалифицирано подписване зависят от софтуера или хардуера, с който се полага електронният подпис, и инфраструктурата на издателя. В Регламента сборът от софтуер и хардуер, който служи за квалифицирано подписване на електронен документ, е описан като „Устройство за полагане на квалифициран електронен подпис“. И четирите нива на подписване са достъпни за всички издадени удостоверения за квалифициран електронен подпис в България, независимо от издателя, но нивата BASELINE_LT и BASELINE_LTA изискват по-високо ниво на софтуера или хардуера, с които се полага електронният подпис, които, разбира се, са свързани с повече разходи и тези нива не са достъпни в повечето безплатни софтуери за подписване. Такъв е примерът с най-популярното софтуерно приложение за електронно подписване – Acrobat Reader.

ЛИТЕРАТУРА

Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар – официален източник https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32014R0910.

Technical Specification ETSI TS 103 172 V2.2.2 (2013-04) by ETSI Technical Committee Electronic Signatures and. Infrastructures (ESI) [viewed 02 August 2024]. Available from: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

Technical Specification ETSI TS 101 733 CMS Advanced Electronic Sigantures (CAdES) [viewed 02 August 2024]. Available from: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf.

Technical Specification ETSI TS 103 171 XML Advanced Electronic Sigantures (XAdES) [viewed 02 August 2024]. Available from: https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.

REFERENCES

1. Reglament (ES) № 910/2014 na Evropeyskia parlament i na Saveta ot 23 yuli 2014 godina otnosno elektronnata identifikatsia i udostoveritelnite uslugi pri elektronni transaktsii na vatreshnia pazar – ofitsialen iztochnik https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32014R0910.

2. Technical Specification ETSI TS 103 172 V2.2.2 (2013-04) by ETSI Technical Committee Electronic Signatures and. Infrastructures (ESI) [viewed 02 August 2024]. Available from:https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.
3. Technical Specification ETSI TS 101 733 CMS Advanced Electronic Sigantures (CAdES) [viewed 02 August 2024]. Available from: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf .
4. Technical Specification ETSI TS 103 171 XML Advanced Electronic Sigantures (XAdES) [viewed 02 August 2024]. Available from: https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.

TITLE SOME ISSUES IN THE LONG-TERM STORAGE OF ELECTRONIC DOCUMENTS SIGNED WITH QUALIFIED ELECTRONIC SIGNATURES

Abstract: *Electronic documents are an essential and integral part of today's digital world. The rapid use of electronic documents in recent years is due to the savings in time and money compared to paper documents. Electronically signed documents are in use in many countries, with their legal value and reliability being ensured by electronic signatures. Qualified electronic signatures (QES) provide the highest level of legal security and are equivalent to a handwritten signature. Qualified electronic signatures are created on the basis of a digital certificate, which is however issued for a certain period of time, and after this period, in order to retain their legal validity and reliability, qualified electronic signatures must be maintained through specialized technologies and processes for long-term storage. The inability to verify the qualified electronic signature after the expiry of the certificate, as well as its other attributes, creates numerous obstacles to the use of electronic documents. This article aims to focus on the problems related to the long-term storage of electronic documents signed with a qualified electronic signature and examines in technical terms the possibilities and levels of electronic signatures, in relation to the adopted EU regulations.*
Keywords: *Electronic signature, QES, storage of QES, time stamp, validity of QES, electronic document*

Senior Assist. Prof. Alexander Kirkov, PhD
University of Library Studies and Information Technologies
E-mail: a.kirkov@unibit.bg

Dimo Vodkadzhiev, eng
District Court – Dobrich
E-mail: vodkadzhiev@gmail.com