поставки в досъдебната фаза възниква фигурата на заподозрения. Най-малкото защото терминологично е по-точно и естествено при наличието на подозрение да говорим за заподозрян, а на обвинение – за обвиняем. При това положение фигурата на обвиняем в досъдебното производство ще възниква едва с изготвянето на обвинителния акт от прокурора или с формулирането на обвинението срещу него отново от прокурора в постановлението, с което предлага освобождаване от наказателна отговорност с налагане на административно наказание или в споразумението (и именно по това обвинение обвиняемият ще се признае за виновен и ще се споразумява). Това ще изисква съответните промени в особените правила по гл. 28 и гл. 29 НПК, но те нито ще са съществени, нито фундаментално проблемни. Повдигането на обвинение и конституиране на фигурата на обвиняемия единствено от прокурора ще е и в пълно съответствие с Конституцията на Р България (КРБ), тъй като според чл. 127, т. 3 КРБ именно прокурорът привлича към отговорност лицата, които са извършили престъпления, и поддържа обвинението по наказателни дела от общ характер. Чл. 128 КРБ предвижда за следствените органи само да осъществяват разследване по наказателни дела в случаите, предвидени в закон. Това на още по-голямо основание важи за останалите разследващи органи, извън следователите, и означава, че те могат да извършват действия по разследване, т.е. действия за събиране на доказателства, но не и да привличат обвиняем (макар да съм наясно, че КС тълкува по друг начин разпоредбите на КРБ и НПК). Заподозреният трябва да има правата на сегашния обвиняем, като там където директивите изискват тези права да се разширят (например по отношение на непълнолетните), това следва да бъде направено.

Това, според мен, е един напълно разумен и възможен подход, макар и очертан в най-общи линии, чрез който можем да транспонираме директивите и производствата за установяване на нарушение от страна на ЕК срещу България ще бъдат прекратени, без да „утежняваме“ досъдебното производство. За реализацията му обаче са нужни сериозни законодателни усилия, които вече не могат да се отлагат. ❑

Кореспондират ли различните файлови формати на електронно подписаните документи на изискванията на Регламент (ЕС) № 910/2014 на Европейския парламент на Съвета на Европа

Д-р Александър Кирков,
Унибит*

Инж. Димо Водкаджиев **
Окръжен съд – Добрич

Резюме: Квалифицираните електронни подписи (QES) са равносилни на собственоръчния подпис и в това отношение имат значителна правна сила. Електронните документи за разлика от хартиените обаче могат да бъдат представени в различни файлови формати и това поражда някои технически и организационни трудности. В тази статия ще разгледаме възможността за електронно подписване на електронните документи в различни файлови формати спрямо приетите в ЕС нормативни документи. Ще бъде разгледано дали различните файлови формати имат предимства или недостатъци в технически аспект при електронно подписване.

Ключови думи: електронен подпис; валидация на електронен подпис; електронен документ; файлов формат

* **Д-р Александър Кирков** е завършил „Технологии“ в СВУБИТ и магистърска програма „Информационна сигурност“. От 2010 година е регистриран съдебен експерт в областта на „Информационните Технологии“ към Софийски градски съд. Асистент в Катедра „Компютърни науки“ към УниБИТ. Член на International Association of Financial

Do the different file formats of electronically signed documents correspond to the requirements of Regulation (EU) No. 910/2014 of the European Parliament of the Counsil of Europe

Alexander Kirkov, PhD, ULSIT

Eng. **Dimo Vodkadzhiev**, DC - Dobrich

Abstract: Qualified electronic signatures (QES) provide the same legal validity as a handwritten signature and in this respect have significant legal force. However, electronic documents, unlike paper documents, can be presented in different file formats, which poses some technical and organizational difficulties. In this article, we will research the possibility of electronically signing on electronic documents in different file formats in relation to the regulatory framework adopted in the EU. It will be researched whether the different file formats have technical advantages or disadvantages in electronic signing.

Keywords: electronic signature; validation of electronic signature; electronic document; file format; digital signature

Въвеждането на електронното подписване и особено законовото приравняване на Квалифицирания електронен подпис към ръчно положения такъв промениха начина, по който осъществяваме подписването на документи. С навлизането на дигитализацията, електронните подписи предлагат значителни преимущества в сравнение с полагането на традиционните подписи.

Въведение С въвеждането на Регламент (ЕС) №910/2014 на Европейският парламент и съвета на Европа бяха въведени и унифицирани нормативни и технически изисквания към електронните подписи в ЕС, като една от постигнатите с това цели е налагането на строги правила за допустимите формати на електронните подписи, което от своя страна повиши сигурността на подписните документи в смисъла на киберсигурността. Същевременно бяха публикувани технически стандарти, което широко разпространи възможността за интегриране на електронно подписване в множество софтуерни продукти, които имат различни изходни файлови формати.

Изхождайки от това, следва, че не винаги файловият формат на създадения изходен файл, съдържащ подписания документ отговаря на техническите спецификации на описаните в стандарта файлови формати, е необходимо да се прави преценка за сигурността на подписания документ и ефективността на ползването на различни файлове формати.

След първоначалния ентусиазъм и подписването на различни по вид електронни документи, бяха детайлизирани европейските стандарти за да позволяват пълно интегриране на електронните подписи в документи.

Допустими формати за електронно подписване

В изпълнение на втората най-важна цел на Регламента – „(2) Целта на настоящия регламент е да се повиши доверието в електронните трансакции на вътрешния пазар, като се предостави обща основа за надеждно взаимодействие по електронен път между гражданите, предприятията и публичните органи, чрез което ще се увеличи ефективността на обществените и частните онлайн услуги, електронния бизнес и електронната търговия в Съюза.“, а именно възможност самите подписи да могат да бъдат проверявани от разстояние, поради това, че едно от най-важните предимства на електронно подписаните документи за надеждно взаимодействие по електронен път между гражданите, предприятията и публичните органи е именно проверката им от разстояние за тяхната автентичност.

За да разберем, има ли значение в какъв формат ще бъде файла на подписания документ, трябва да разгледаме допустимите формати за електронно подписване, които са представени в стандарта Procedures for Creation and Validation of AdES Digital Signatures (ETSI EN 319 102) свързан с Регламент 910/2014, където са описани съответните формати за електронно подписване, познати като: XAdES, CAdES и PAdES, а техните подробни технически спецификации за посочени в следните документи:

Crimes Investigators (IAFCI), International Association of Computer Investigative Specialists (IACIS) и на ISACA Serving IT Governance Professionals.

** **Димо Водкаджиев** е завършил специалност „Електронна техника и микроелектроника“ в Технически университет – Варна. От 2006 година е системен администратор последователно в Районен съд – Генерал Тошево и впоследствие в Окръжен съд – Добрич. Лектор съм към различни органи на съдебната власт в прилагане на образователните програми на Висшия съдебен съвет.

• Technical Specification XML Advanced Electronic Sigantures (XAdES) - ETSI TS 103 171

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

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

Съществуват и други формати за подписване, но те са предназначени за подписване на друг тип данни и файлове.

XAdES

XAdES е стандарт за усъвършенстван електронен подпис, който се базира на **XML** (eXtensible Markup Language) формат на файла и е разработен от **ETSI** (European Telecommunications Standards Institute). Целта на XAdES е да осигури правна сигурност и дългосрочна защита на електронните подписи в формат на данните XML.

Форматът на данните/файловете XML е структуриран и четим както за машини, така и за хора, като същевременно осигурява автентичност и цялостност на данните във файла. Например, популярните софтуери за обработка на документи: MS Word и MS Excel могат да отварят и да записват XML файлове (Open XML).

Изходният файлов формат на данните/файловете съдържащи положен електронен подпис (разширението на подписан файл) в контекста на XAdES е единствено .xml, като се поддържат типове подпис: “ENVELOPED” и “DETACHED”.

• **ENVELOPED XAdES** е електронно подписване, при което данните на електронния подпис се интегрират в самият XML файл. Този вид подписване може да бъде приложен само за унифицирани XML файлове.

• **DETACHED XAdES** е електронно подписване, при което данните на електронния подпис се поставят в друг файл и не променят оригиналния файл. Този начин на подписване може да бъде приложен и за други видове файлове, но той е труден за проверка, тъй като процедурата е еднопосочна и липсва пряка връзка между оригиналния и файла съдържащ подписа. Във файла съдържащ електронния подпис не се съдържа информация за оригиналния файл, а само резултата от математическата проверка на този файл – HASH сума. По този начин, единствената проверка, която може да се направи е, да се сравнят чрез специализиран софтуер

оригиналният и файлът с подписа, дали ще бъде отново изчислена стойност на Hash сумата, която да съвпадне с тази във файла с подписа.

Предимството на електронното подписване на файлове във XML формат е това, че тези файлове са лесни за машинна обработка. Те са предпочитани за случаите, когато трябва да се поставя електронен печат и печат с точно време или за автоматично издаване или обработка на документи, например електронни деловодни системи.

Недостатък на подписването ENVELOPED XAdES, е че се използва интегриране на подписаните данни като част от подписания файл, които се изразяват с програмни оператори и това е пречка за хора без специализирани знания да проверят поставеният електронен подпис.

CAdES

CAdES е стандарт за усъвършенствани електронни подписи, разработен от **ETSI** (European Telecommunications Standards Institute), който използва **CMS** (Cryptographic Message Syntax) като базов формат за подписване. CAdES е предназначен да осигури усъвършенствани и квалифицирани електронни подписи, които отговарят на изискванията на **eIDAS** регламента за правна сила и сигурност.

Подобно на XAdES, CAdES също фокусиран върху предоставянето на сигурно ниво на електронно подписване гарантиращо цялостност, автентичност и правна стойност, като предлага гъвкавост при подписване на различни видове файлове.

Основните срещани формати на документи/файлове, подписани с CAdES, са .p7s и .p7m, както следва:

• **P7S (PKCS#7 Signed Data) формата** съдържа подписа и допълнителна информация за сертификата и метаданни за подписа. При този файлов формат типа на подписа е “DETACHED” тоест подписаното съдържание и самият подпис са в отделни файлове. Самият файл с разширение .p7s **не съдържа подписаните данни** той съдържа само подписа, който трябва да бъде проверен/валидиран заедно с подписаното съдържание. И както описахме за DETACHED XAdES, този тип подпис е труден за проверка, тъй като процедурата е еднопосочна и липсва пряка връзка между оригиналния и файла съдържащ подписа.

• **P7M (Signed Message with Attached Content)** формата съдържа както подписа, така и самото подписано съдържание – тип на подписа "ENVELOPING/ATTACHED". Този вид подписване е подходящ за случаи, когато се изисква подписът и съдържанието да бъдат изпратени заедно, като не е необходимо външно свързване на данните с подписа. Недостатъците на този тип подписване са, че потребителите се нуждаят от специфичен софтуер за цифров подпис, за да отворят p7m файла, в случай на множество подписи върху един и същ документ потребителите трябва да подписват последователно p7m файла за всяко прикрепване (създаване на така наречения ефект на матрьошка), което не позволява да се видят всички подписи едновременно, а също така този тип подписване не позволява добавяне на видим графичен подпис върху документа.

PAdES

PAdES е стандарт за усъвършенствани електронни подписи, който използва PDF (Portable Document Format) като контейнер за подписване. Разработен от ETSI (European Telecommunications Standards Institute), този стандарт е съвместим с изискванията на eIDAS регламента и е предназначен да осигури правна стойност и дългосрочна валидност на електронните подписи, когато се прилагат към PDF документи.

Подобно и на предните два разгледани формата, PAdES предлага високо ниво сигурност и автентичност на подписаните документи, като включва нужните механизми за: цялостност на данните, автентичност на подписващия и възможност за непрекъсната валидност на подписа.

При формата PAdES електронният подпис се вгражда в самия PDF документ и всички подписани документи/файлове се съхраняват само и единствено в PDF формат.

Важно е да се отбележи, че подписаните файлове запазват пълната си съвместимост с всички стандартни програми за преглед на PDF документи. (не само с например Acrobat Reader). Това е един от големите плюсове на формата, защото подписаният документ остава лесно четим и позволява лесното му споделяне без нужда от допълнителен софтуер, което е особено полезно при правни и административни документи.

Друго голямо предимство на PAdES формата е, че позволява многократно подписване на един и същ PDF документ. Например, когато няколко души трябва да подпишат един документ, всеки подпис може да бъде добавен последователно, без да се нарушава валидността на предишните подписи.

Има възможност при полагане на подпис, документът да бъде финализиран, заключен за по нататъшни промени или подписи.

Положеният електронен подпис при PAdES формата има възможност да бъде вграждан в различни части на документа, като същевременно има и възможност подписите да бъдат положени като видими или невидими, като при първите се визуализира знак или текст за положения подпис. Дали подписите са видими или невидими е възможност която се избира от полагащия електронния подпис.

Правна регламентация на валидирането на поставените електронни подписи

На практика в Регламент 910/2014 на ЕП и Съвета, не са посочени ограничения за подписването в конкретен формат, обаче на практика се оказва, че не всички разработени стандарти и технически спецификации за електронно подписване са придобили широко разпространение и съответно не за всички формати има разработен технически инструментариум, като софтуери за подписване и проверка на подписани документи.

За тези формати, които поради липсата на стандарт и подробна техническа спецификация, ще бъде свързано с трудност подписаните електронни документи да бъдат проверявани от разстояние, както и, като цяло ще бъде трудно да бъдат проверявани за сигурност и автентичност. Същото на практика важи и за формате на данни, за които стандартите за подписване не са широко разпространени и за тях липсват изградени лесно достъпни софтуери. В т. 2 от чл. 32 на Регламент 910/2024 г, ясно е посочено изискването, че използваната за валидиране на квалифицирания електронен подпис система предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността, а в буква б) т. 1 на чл. 33 от същия регламент е записано задължението, че дава възможност на доверяващите се страни да получат резултата от процеса на валидиране по автоматизиран начин, който е

надежден и ефикасен и носи усъвършенстван електронен подпис или усъвършенстван електронен печат на доставчика на услугата по квалифицирано валидиране, което на практика означава, че валидирането (проверката) на поставените електронни подписи трябва да се извършва от квалифициран специалист или от софтуер, който е разработен за тази цел и отговаря на поставените изисквания в Регламента.

На национално ниво в Закона за електронния документ и електронните удостоверителни вериги също няма изрично указани методи и инструментариум за проверка на положени електронни подписи. Струва си да се отбележи, чл. 28 на „Наредба №6 За извършване на процесуални действия и удостоверителни изявления в електронна форма" на Висшия съдебен съвет, където в подкрепа на написаното в т. 1 на чл. 33 на Регламент 910/2014 изрично е указано проверките на електронните документи включително и валидирането на положени в тях електронни подписи да става по автоматизиран начин.

В технологичен аспект, софтуерните продукти, извършващи валидиране на електронни подписи трябва да бъдат верифицирани, че изпълняват правилно и пълноценно валидациите, за да може да се ползват с доверие, независимо, че ЕК не е посочила конкретни технически стандарти за процедурата по валидиране на електронно подписан документ, то такава практика вече съществува в други подобни области и процедури по верифициране и валидиране на работата на съответни софтуери, се правят по съществуващите стандарти за управление на качеството, а именно БДС/ISO 9001 и стандарти за управление на сигурността – БДС/ISO 27001.

В този смисъл, липсата на надеждни софтуери за проверка на електронно подписани документи, без значение, дали те са във файлов формат различен от популярните формати за електронно подписване или в не-стандартизиран от ETSI формат, ще доведе до трудности при валидирането на документите и съответно до ниска ефективност.

Софтуер за подписване

Поради широкото разпространение и лесното използване, най-популярният софтуер за подписване е **Acrobat Reader**, на дружеството Adobe – САЩ. Този софтуер е популярен не само в България, той се използва от държавна и общинска администрация и вероятно по тези причини е сертифициран по редица международни стандарти, като: SOC 2–Type 2 (Security, Availability, & Confidentiality), SOC 3 (Security, Availability, & Confidentiality), ISO 27001:2022, ISO 27017:2015, ISO 27018:2019, ISO 22301:2019 ,C5 Certified (Germany), FedRAMP Tailored, ISMAP Registered (Japan), GLBA ready [1], FERPA ready [1].

Разбира се, трябва да уточним, че за pdf формат на файла и за PAdES подписване има много софтуери, които са безплатни и работят добре, Acrobat Reader не е единственият такъв, той просто е най-популярният.

Microsoft Word е също много популярен софтуер за подписване в много държави, но тъй като по подразбиране, той е настроен да работи със удостоверения за електронни подписи, издадени онлайн, е необходимо да бъде допълнително настроен, за да може да се ползва с такива издадени по eIDAS (Регламент 910/2014). Без да бъдат направени тези настройки, подписаните документи не се подписват правилно или не могат да бъдат проверявани, ако се подписват с издавани у нас удостоверения.

Други недостатъци на Microsoft Word, е работата с големи документи или когато са необходими множество подписи в един документ. Неговите мерки за сигурност не винаги са подходящи спрямо изискваното ниво за КЕП. И не на последно място, самият Word не може да валидира напълно електронно подписан документ, както и за този формат вече няма много софтуери, които да валидират интегрираните в него електронни подписи, и това също прави подписването чрез него непопулярно и слабоефективно.

DocuSign е друг придобил популярност софтуерен инструмент за подписване. Той е специално проектиран за цифрово подписване и разполага с широк набор от функции, пригодени за тази цел.

DocuSign технологично представлява цифров облак и е лесен за използване, както и има стабилни мерки за сигурност. Потребителите лесно да качват, подписват, споделят и изтеглят документи. Той използва криптиране, за да защити записаните в него документи и подписи.

Недостатъците на DocuSign са няколко: основно той е предназначен за използване в САЩ и Великобритания и е съобразен с техните правни изисквания и практики. Също така, той предоставя услугите си срещу абонаментна такса.

По посочените по-горе причини, най-честата практика в

България е, електронните документи да се изготвят чрез Microsoft Word, в последствие да се конвертират във формат pdf и да се подписват с Acrobat Reader. По този начин се използва лесният интерфейс на Word и се избягват ограничените възможности на Acrobat Reader за работа с документи.

Подписването на електронен документ в Word и в последствие конвертирането му заедно с подписа в pdf на теория е възможно, но на практика е невъзможно да се направи така, че да се запази електронният подпис, като функционалност.

В заключение В Регламент 910/2014 година и техническите стандарти и спецификации към него са допустими множество формати на файловете за електронно подписване. На практика в самия Регламент не се поставят граници за това, само за шест от тях има разработени подробни технически спецификации. На този етап, само два са най-често ползваните формати на файловете, които се ползват за електронно подписване в България, поради това, че съществуват множество софтуери за подписване и валидация на този вид файлове.

За популярните формати (CAdES и PAdES) са създадени софтуерни системи за квалифицирано валидиране, което позволява лесно и без нуждата на експерти да бъдат проверявани подписаните електронни документи, докато за другите описани в стандарта формати, а също така и за неописаните, такива системи няма или те не са проверени и съответно доверени. При допускане на такива документи, ще бъде необходимо да се изготвя експертно становище, тъй като не съществува друг начин на валидиране на подписите, а експертното становище ще забави и оскъпи процеса на приема на електронния документ.

От посочените по-горе причини, се налага изводът, че държавната, общинска и съдебна администрация трябва временно да ограничи допускането на електронно подписани документи, до форматите за които бързо, лесно и надеждно може да се валидира подписаният документ . На този етап това са форматите допустими за CAdES или PAdES подписване, а останалите формати да не бъдат приемани. Друг компромисен вариант би могъл да бъде, като за подаване на електронни документи във файлов формат различен от допустимите за CAdES или PAdES, да бъде предвиждано допълнително време за валидация на документите. ❑

Коментар

Сключването на договор за управление като основание за уволнение на служителите от ръководството на предприятието

Част I

Гл. ас. д-р Христо Банов*

Резюме: В научното изследване е детайлно анализирано сключването на договор за управление като основание за прекратяването на трудовите договори със служителите от ръководството на предприятието. Във връзка с това задълбочено са разгледани въпросът относно правното значение на изпълнението на договора за управление, както и проблемите относно точния момент, в който започва да тече максималният 9-месечен срок за упражняване на указаното право на уволнение, за кръга на служителите, които попадат в ръководството на предприятието и др. Обърнато е внимание на допълнителните изисквания, произтичащи от специалната уредба на публичните предприятия, за законосъобразност на уволнението на служителите от ръководството на публично предприятие при сключването на договор за управлението му. Посочени са и особеностите на уволнението на основание чл. 328, ал. 2 от Кодекса на труда при сключването на договор за управление на висше училище между ректора на последното и министъра образованието и науката.

Ключови думи: безвиновно основание за уволнение; сключване на договор за управление; Търговски регистър и регистър на юридическите лица с нестопанска цел; Регистър БУЛСТАТ; 9-месечен срок за упражняване на правото на уволнение; управител; служители от ръководството на предприятието; ръководство на поделение на предприятието; длъжностни лица; конкурс за управител на публично предприятие; бизнес задача; бизнес програма; ректор; висше училище

* **Христо Банов** е главен асистент по трудово право и обществено осигуряване в Института за държавата и правото при Българската академия на науките, преподавател по трудово и осигурително право в Правно-историческия факултет на Югозападния университет „Неофит Рилски“. Доктор по право. Адвокат – член на Софийската адвокатска колегия.