Univerzita Karlova v Praze

Právnická fakulta

Elektronický podpis v právu EU

Studentská vědecká a odborná činnost

Kategorie: magisterské studium

2014 Autor: Ing. Filip Stuna

VII.ročník SVOČ

Čestné prohlášení a souhlas s publikací práce

Prohlašuji, že jsem práci předkládanou do VII. ročníku Studentské vědecké a odborné činnosti (SVOČ) vypracoval samostatně za použití literatury a zdrojů v ní uvedených. Dále prohlašuji, že práce nebyla ani jako celek, ani z podstatné části dříve publikována, obhájena jako součást bakalářské, diplomové, rigorózní nebo jiné studentské kvalifikační práce a nebyla přihlášena do předchozích ročníků SVOČ či jiné soutěže.

Souhlasím s užitím této práce rozšiřováním, rozmnožováním a sdělováním veřejnosti v neomezeném rozsahu pro účely publikace a prezentace PF UK, včetně užití třetími osobami.

V Praze dne 15.4.2014

…….……..

Ing. Filip Stuna

Obsah

1 Úvod

Překotný vývoj IT technologií v posledních desetiletích znamenal zásadní změnu způsobu práce v mnoha odvětvích lidské činnosti. V současnosti již lze těžko v našem prostředí najít firmu, která není vybavena počítačem a nezpracovává alespoň část agendy elektronicky. S rozvojem internetu se stala běžnou elektronická komunikace – mezinárodní, globální. Společně s internetem a elektronickou komunikací se rozvíjel i elektronický obchod. Od transakcí probíhajících v reálném čase, jako je nákup a prodej na trhu s cennými papíry, přes internetové obchody nabízející spotřební zboží, až po sjednávání obchodních dohod, jejichž předmět a podmínky uskutečnění jsou zakotveny ve smlouvách a jejichž doba naplňování a platnosti může trvat řádově až desítky let. Jedním takových dlouhodobých kontraktů jsou například úvěrové smlouvy mezi bankami a jejich klienty, které jsou uzavřeny tzv. „na dálku“, tedy bez fyzické přítomnosti klienta v bance, a dokonce jsou uzavřeny pouze v „nepapírové“, tedy digitální podobě.

V závislosti na finančním ohodnocení transakce nebo důsledků z takové transakce vyplývajících, je záhodno snížit adekvátně rizika, která plynou z možnosti nedodržení smluvních podmínek jednou ze smluvních stran. Kromě finančních nástrojů, využívaných při řízení rizik, je to také nástroj, který má oporu v právním řádu Evropské unie a České republiky a umožňuje i bez osobního kontaktu prokázat, že příslušná smluvní strana náležitě uzavřela elektronickou smlouvu a vyjádřila tak svoji vůli. Jedná se o elektronický podpis.

Jde o pojem, který se v posledních letech dostal i do širšího povědomí veřejnosti v ČR, zejména v souvislosti s projekty elektronizace veřejné správy, z nichž tím nejznámějším je zřejmě Informační Systém Datových Schránek (ISDS). Elektronický podpis je založen na matematických a IT metodách, popsaných na počátku 70. let 20. století. Použití těchto metod umožňuje, aby byla k datové zprávě (což může být elektronická smlouva, elektronický úřední formulář nebo jakýkoliv jiný počítačový soubor) připojena data (podpis), pomocí kterých lze zajistit integritu datové zprávy a nepopiratelnost, respektive neodmítnutelnost odpovědnosti za tento vytvořený „podpis“. Právě nepopiratelnost elektronického podpisu je odvozena z legislativní opory, která má svůj původ v právu EU.

Cílem této práce je popsat vývoj a současný stav legislativy EU týkající se elektronického podpisu, nastínit její pravděpodobný vývoj v blízké budoucnosti a zmínit způsob, jakým je příslušná evropská legislativa naplněna v českém právním řádu.

Jelikož se jedná o problematiku těsně svázanou se specifickými matematickými a IT metodami, je dle autora pro pochopení souvislostí nezbytné na úvod alespoň stručně vysvětlit základní technické pojmy a způsob fungování elektronického podpisu. Vzhledem ke stanovenému rozsahu práce bylo nutno omezit šíři a detail technického popisu pouze na základní pojmy a nebylo možné vyhnout se některým zjednodušením.

Rovněž v pasážích věnujících se legislativě je z důvodu udržení požadovaného rozsahu práce pozornost věnována výhradně elektronickému podpisu, ač třeba příslušné právní úpravy řeší i další blízce související témata.

Práce čerpá z veřejně dostupných zdrojů, které jsou uvedeny u příslušných citací nebo v seznamu literatury. Dále autor využívá svých osobních zkušeností a znalostí, které získal, když se jako zaměstnanec společnosti První certifikační autorita, a.s., podílel na projektech implementujících elektronický podpis u zákazníků společnosti.

2 Základní technický popis

Elektronický podpis splňující základní požadavky legislativy, která je popsána v této práci, je založen na matematických metodách asymetrické kryptografie. To znamená, že se zde používá dvojice klíčů (digitálních řetězců), která musí splňovat následující vlastnosti[1]:

- je jednoznačná – vygenerována náhodně, nepredikovatelně a s vysokou mírou pravděpodobnosti, že nebude v dohledné době vygenerován další stejný pár klíčů,
- jeden klíč z druhého nelze odvodit,
- data zašifrovaná jedním klíčem, lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů.

Praktické použití je takové, že jeden z klíčů zůstává pod výhradní kontrolou majitele klíče a takový klíč se označuje jako „**soukromý klíč**“. Druhý z páru klíčů se zveřejní a takový klíč se nazývá „**veřejný klíč**“.

V souvislosti s tímto pojmem se ve světě informačních technologií nazývá množina prvků systému, který umožňuje fungování elektronického podepisování na principu veřejného klíče, infrastrukturou správy a distribuce veřejných klíčů, neboli **PKI**[2].

Aby bylo zřejmé, kdo je uživatelem páru klíčů, spojí se veřejný klíč s údaji o uživateli (jméno, příjmení, atd.) do datové struktury, která se nazývá **certifikát**. Pro úvodní představu si lze certifikát představit jako záznam v telefonním seznamu: telefonní číslo coby veřejný klíč vlastníka a údaje k telefonnímu číslu připojené (jméno, adresa) pak jako položky v certifikátu identifikující vlastníka certifikátu. Certifikát je ale podstatně složitější struktura než záznam v telefonním seznamu a obsahuje kromě zmíněných položek i další, z nichž některé jsou v certifikátu uváděny povinně (datum vydání certifikátu, doba platnosti, atd.) a některé jsou volitelné (například akademický titul vlastníka).

[1] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008. s. 34.
[2] z anglického Public Key Infrastructure

Certifikáty vydává **certifikační autorita**. Certifikační autorita je pojem, kterým je v oblasti PKI možné popsat třetí důvěryhodnou stranu, instituci nezávislou na komunikujících stranách, které využívají její certifikáty.

Aby bylo možné dokončit popis principu vytváření elektronického podpisu, zbývá vysvětlení termínu „hash“. **Hash** je jednocestná matematická funkce, která z libovolně velkých dat vypočítá krátký řetězec konstantní délky – hash hodnotu (nebo také pouze **hash**). Kvalitní hash funkce by měla splňovat tři podmínky:

- Odolnost vůči získání předlohy – z dané hash hodnoty nelze získat původní zprávu, jedná se o jednocestnou funkci.
- Odolnost vůči získání jiné předlohy – pro danou hash hodnotu je prakticky nemožné najít jinou zprávu, jejíž hash hodnota odpovídá hash hodnotě původní zprávy.
- Odolnost vůči nalezení kolize – je prakticky nemožné najít dvě zprávy se stejnou hash hodnotou.

Elektronický podpis[3] náležející k nějaké datové zprávě je tedy ve svém nejjednodušším tvaru takováto hash hodnota vypočítaná z příslušné datové zprávy a zašifrovaná soukromým klíčem. Takto zašifrovaná hash se nazývá **kryptogram**.

V odborné literatuře lze nalézt pojmy „elektronický podpis“ i „digitální podpis“. Význam těchto dvou pojmů se někdy rozlišuje tak, že elektronický podpis je širší pojmenování pro jakékoliv údaje v elektronické podobě připojené k dokumentu a mající povahu podpisu a digitální podpis je pak podmnožinou elektronického podpisu a je to elektronický podpis založený na asymetrické kryptografii. V této práci je, stejně jako v běžném použití a ve většině odborné literatury, termín „elektronický podpis“ ekvivalentní pojmu „digitální podpis“.

[3] V odborné literatuře lze nalézt pojmy „elektronický podpis“ i „digitální podpis“. Význam těchto dvou pojmů se někdy rozlišuje tak, že elektronický podpis je širší pojmenování pro jakékoliv údaje v elektronické podobě připojené k dokumentu a mající povahu podpisu a digitální podpis je pak podmnožinou elektronického podpisu a je to elektronický podpis založený na asymetrické kryptografii. V této práci, stejně jako v běžném použití a ve většině odborné literatury, je termín „elektronický podpis“ ekvivalentní pojmu „digitální podpis“. (viz např. PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, c2011. s. 30.)

Princip ověření elektronického podpisu spočívá v tom, že kryptogram je dešifrován veřejným klíčem nalézajícím se v certifikátu a takto získaná původní hash je srovnána s nově vypočtenou hash z příslušného dokumentu.

V případě, že jsou srovnávané hodnoty shodné, má ověřující jistotu, že podepisující podepisoval stejnou zprávu, ke které je ověřován podpis.

Ověřující ví, že veřejný klíč, který použil pro dešifrování podpisu a získání původního hashe, patří k soukromému klíči, kterým byla zpráva podepsána.

Jelikož je veřejný klíč spojen v certifikátu s údaji vlastníka certifikátu, respektive podepisující osoby, může takto osoba ověřující podpis identifikovat podepisující osobu.

Důvěra komunikujících stran v pravdivost údajů obsažených v certifikátu je úměrná důvěře v certifikační autoritu a její postupy při poskytování certifikačních služeb. Nároky na tyto postupy, důvěryhodnost a úroveň služeb vycházejí právě z legislativních požadavků, jejichž splnění umožní certifikační autoritě získat akreditaci pro vydávání certifikátů, jejichž použití a důsledky z tohoto použití jsou upraveny zákonem.

3 Elektronický podpis v právu EU

Díky bezpečnosti technologie asymetrické kryptografie a relativně jednoduchému způsobu distribuce veřejných klíčů za pomoci certifikátů bylo umožněno využití výhod elektronického podpisu v rámci obchodního styku. Nastalou situaci řešily první právní úpravy týkající se použití elektronického podpisu a stanovující určitá pravidla pro participující strany. Tato přijatá legislativa následně umožnila použití elektronického podpisu i v komunikaci mezi občany a orgány veřejné moci.

3.1 Směrnice Evropského parlamentu a Rady 1999/93/ES

V Evropě se stala harmonizujícím prvkem mezi národními legislativami Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 (dále jako 1999/93/ES nebo pouze Směrnice). Směrnice je stále právně závazným dokumentem pro členské státy EU.

3.1.1 Zdůvodnění, cíle

Několik níže uvedených citací bodů z úvodu Směrnice vyjadřuje výstižně záměr, s jakým směrnice vznikla:

- „elektronická komunikace a obchod vyžadují elektronické podpisy a s nimi související služby umožňující autentizaci dat; rozdíly v předpisech členských států týkajících se právního uznání elektronických podpisů a akreditace poskytovatelů certifikačních služeb by mohly vytvořit vážnou překážku používání elektronické komunikace a elektronického obchodu; vytvoření jasného rámce Společenství, který upraví podmínky vztahující se k elektronickým podpisům, posílí důvěru v nové technologie a jejich obecné uznání; legislativa členských států by neměla bránit volnému pohybu zboží a služeb na vnitřním trhu;“ (1999/93/ES, úvod, bod 4)

- „elektronické podpisy budou používány ve veřejném sektoru uvnitř vnitrostátních orgánů a orgánů Společenství a při komunikaci mezi těmito orgány navzájem a mezi těmito orgány a občany a

hospodářskými subjekty, například v oblasti veřejných zakázek, daní, sociálního zabezpečení, zdravotnictví a soudnictví;“ (1999/93/ES, úvod, bod 19)

- „harmonizovaná kritéria týkající se právních účinků elektronických podpisů budou zárukou jednotného právního rámce Společenství; vnitrostátní právní předpisy upravují různé požadavky týkající se právní platnosti vlastnoručních podpisů; pro potvrzení totožnosti osoby, která se elektronicky podepisuje, lze použít certifikáty; zaručené elektronické podpisy založené na kvalifikovaných certifikátech vedou k zajištění vyšší úrovně bezpečnosti; zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené prostředky pro bezpečné vytváření podpisů lze z právního hlediska považovat za rovnocenné vlastnoručním podpisům pouze za předpokladu, že jsou naplněny požadavky na vlastnoruční podpisy;“ (1999/93/ES, úvod, bod 20)

- „aby došlo k obecnému přijetí elektronických autentizačních metod, je třeba zajistit, aby elektronické podpisy mohly být ve všech členských státech používány jako důkazy v soudním řízení; …“ (1999/93/ES, úvod, bod 21)

Cílem Směrnice tedy bylo vytvoření právního rámce pro použití elektronického podpisu a pro poskytování certifikačních služeb[4]. Měla být nastavena transparentní pravidla, která by umožnila v rámci EU volný pohyb produktů a služeb poskytovatelů certifikačních služeb (tedy certifikačních autorit). Dále měla být zajištěna vzájemná bezproblémová uznatelnost elektronických podpisů vytvořených na základě certifikátů vydaných poskytovateli certifikačních služeb v jednotlivých členských zemích EU.

3.1.2 Naplnění cílů Směrnice

Jelikož Směrnice v některých částech neurčovala striktně požadavky ve vztahu k členským státům, měly jednotlivé členské státy volnost při výkladu Směrnice a

[4] Ve smyslu služeb certifikační autority, jak je chápána v oblasti PKI.

aplikaci v lokálních legislativách. Finální implementace doporučení Směrnice v jednotlivých členských státech se tak lišila, což způsobilo vzájemnou omezenou kompatibilitu při uznávání elektronického podpisu.

Zejména se tato skutečnost týkala odstavce 2 a odstavce 7 článku 3 „Přístup na trh“ Směrnice:

„Článek 3 - Přístup na trh

1) Členské státy nebudou poskytování certifikačních služeb podmiňovat autorizací.

2) Aniž by tím bylo dotčeno ustanovení odstavce 1, mohou členské státy zavést nebo ponechat v platnosti dobrovolné akreditační systémy, jejichž cílem je zvýšit úroveň zajišťování certifikačních služeb. Veškeré podmínky spojené s těmito systémy musí být objektivní, transparentní, úměrné a nediskriminační. Členské státy nesmí omezovat počet akreditovaných poskytovatelů certifikačních služeb z důvodů, které spadají do působnosti této směrnice.

...

7) Členské státy mohou používání elektronických podpisů ve veřejnoprávním sektoru podmínit případnými doplňujícími požadavky. Tyto požadavky musí být objektivní, transparentní, úměrné a nediskriminační a musí se vztahovat výlučně na specifické vlastnosti daného použití. Tyto podmínky nesmějí vytvářet překážky pro přeshraniční služby.“

Ing. Jaroslav Tománek k tomu ve své diplomové práci „Problematika přeshraničního uznávání elektronických podpisů“[5] poznamenal:

„Těchto ustanovení využila většina členských států a podle odstavce 2 (a tedy v souladu se směrnicí) pro poskytovatele certifikačních služeb vytvořila dobrovolná akreditační schémata. Podle odstavce 7 potom zákonem podmínila užití elektronického podpisu při komunikaci v rámci veřejnoprávního sektoru použitím elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Tento model se stal velmi

[5] Tománek, J. Problematika přeshraničního uznávání elektronických podpisů. (Diplomová práce) Praha: ČZÚ, 2011. s 46.

rozšířeným (přestože by se dalo úspěšně polemizovat o jeho objektivnosti, transparentnosti a nediskriminačnosti) a byl hlavní příčinou nestejnorodých právních úprav členských států, z kterých plynou velmi přísné, nebo naopak velmi shovívavé požadavky na poskytovatele certifikačních služeb, a tím i značně rozdílné požadavky na elektronický podpis v oblasti veřejnoprávního sektoru v jednotlivých členských státech.“

Uvedený stav nejenže zkomplikoval volný pohyb zboží služeb, ale komplikoval také možnost ověření zaručeného elektronického podpisu vytvořeného pomocí kvalifikovaného certifikátu, který byl vydaný zahraničním poskytovatelem certifikačních služeb.

Praktický dopad tohoto stavu nebyl ten, že by zákazníci rezignovali na použití elektronického podpisu, ale například si pro elektronickou komunikaci s úřady opatřovali kvalifikovaný certifikát u poskytovatele certifikačních služeb v příslušném státě.

I přes tyto problémy lze konstatovat, že významným přínosem Směrnice bylo zavedení legislativy týkající se elektronického podpisu členskými státy a definice jednotného pojmosloví, které členské státy ze Směrnice převzaly.

3.1.3 Definice pojmů

Nutno podotknout, že ačkoliv jsou ve Směrnici použity pojmy z oblasti PKI a de facto znění Směrnice vychází z principů fungování PKI, zachovává si Směrnice technologickou neutralitu, aby umožnila použití nových technologií, které by splňovaly její podmínky.

Jako příklad lze uvést několik zásadních pojmů z české legislativy, která naplňuje Směrnici, konkrétně ze Zákona č. 227/2000 Sb. o elektronickém podpisu §2:

„Pro účely tohoto zákona se rozumí

a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě,

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

…

g) držitelem certifikátu fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán,

h) poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

i) kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,

j) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

k) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,

l) kvalifikovaným certifikátem certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

….

n) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,

o) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,

…“

3.2 Rozhodnutí Komise 2009/767/ES

V souvislosti s evropskou směrnicí 2006/123/ES o službách na vnitřním trhu, jejímž cílem bylo odstranit administrativní překážky pro poskytování služeb v členských státech a naplnit tak zásadu svobody pohybu, která je základem společného trhu EU, vyvstala opět potřeba přeshraničního uznávání zaručených elektronických podpisů, resp. kvalifikovaných certifikátů.

Dne 16. října 2009 bylo přijato rozhodnutí Komise 2009/767/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu, které nabylo účinnosti dne 28. prosince 2009.

Členské státy tímto rozhodnutím dostaly za povinnost uvést do provozu TSL (Trusted Services List), což je seznam kvalifikovaných poskytovatelů certifikačních služeb, kteří jsou v daném státu akreditování, resp. je nad nimi vykonáván dozor. Dále má být na TSL seznam služeb, kteří tito poskytovatelé poskytují a jejich historie.

Jednotlivé státy tedy vytváří vlastní TSL a Evropská komise zveřejňuje seznam adres všech publikovaných TSL členských států v „seznamu TSL“ (LOTL - List of the Lists), který uveřejňuje v lidsky čitelné podobě (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf)

nebo ve strojově zpracovatelné podobě (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml).

Pro potřeby ověření zaručeného elektronického podpisu tak vznikl jakýsi „evropský seznam poskytovatelů vydávajících kvalifikované certifikáty a jejich služeb“.

3.3 Rozhodnutí Komise 2010/425/EU

Tímto rozhodnutím byly napraveny některé nedostatky předchozího rozhodnutí Komise 2009/767/ES. Jedná se tak v podstatě o jeho novelu.

Členským státům byly v souvislosti s TSL uloženy nové povinnosti[6]:

- publikovat jak lidsky čitelnou (ve formátu PDF), tak strojově zpracovatelnou (ve formátu XML) podobu TSL,
- strojově zpracovatelná podoba musí být elektronicky podepsána,
- lidsky čitelná podoba musí být publikovaná bezpečným způsobem (tj. zabezpečeným kanálem pomocí protokolu SSL/TLS nebo elektronicky podepsaná),
- členské státy jsou povinny předat Evropské komisi veřejné klíče potřebné k ověření podpisů TSL a ta následně zajistí jejich důvěryhodnou distribuci přes centrální seznam TSL (LOTL).

3.4 Rozhodnutí Komise 2011/130/EU

25. února 2011 vydala EK rozhodnutí 2011/130/EU, které nabylo účinnosti 1. srpna 2011. Toto rozhodnutí pokračovalo v naplňování směrnice 2006/123/ES a uložilo členským státům tyto nové povinnosti:

1. *Členské státy zavedou nezbytné technické prostředky, které jim umožní zpracování elektronicky podepsaných dokumentů, jež v rámci plnění postupů a formalit předkládají poskytovatelé služeb prostřednictvím jednotných*

[6] Tománek, J. Problematika přeshraničního uznávání elektronických podpisů. (Diplomová práce) Praha: ČZÚ, 2011. s 59.

kontaktních míst, jak je stanoveno v článku 8 směrnice 2006/123/ES, a které jsou podepsány příslušnými orgány jiných členských států pomocí zaručeného elektronického podpisu XML nebo CMS nebo PDF ve formátu BES nebo EPES, který je v souladu s technickými specifikacemi uvedenými v příloze.

2. *Členské státy, jejichž příslušné orgány podepisují dokumenty uvedené v odstavci 1 za použití jiných formátů elektronických podpisů, než jsou uvedeny v odstavci 1, oznámí Komisi stávající možnosti ověření, které umožní ostatním členským státům ověřit obdržené elektronické podpisy online, bez poplatku a způsobem, který je srozumitelný pro nerodilé mluvčí, pokud požadované informace nejsou již zahrnuty v dokumentu, elektronickém podpise nebo nosiči elektronického dokumentu. Komise zpřístupní tyto informace všem členským státům.*

Toto rozhodnutí bylo dalším posunem, kterým se zvýšila právní jistota týkající se elektronického podpisu v přeshraničním uznávání.

Komise zvolila tři různé formáty elektronického podpisu:

- podpis CMS (Cryptographic Message Syntax, definovaný ve standardu RCF 5652) ve formátech CAdES-BES/EPES, definovaných v ETSI TS 101 733,
- podpis XML ve formátech XAdES-BES/EPES, definovaných v ETSI TS 101 903,
- podpis PDF ve formátech PAdES-BES/EPES, definovaných v ETSI TS 102 778.

Každý orgán veřejné moci musí tak být schopen zpracovat všechny tři formáty, pro podpis musí být používán jeden z těchto formátů. Pokud orgán veřejné moci používá jiný formát, musí příslušný stát zveřejnit zdarma online aplikaci pro ověřování, která umožní srozumitelně i pro cizince ověřit elektronické podpisy na dokumentech pocházejících z této země.

Velký význam však toto rozhodnutí mělo i pro tuzemské sjednocování přístupu k elektronickému podpisu, jelikož se ve své příloze odkazovalo na konkrétní

formáty elektronických podpisů, což umožnilo výrobcům aplikací určených k elektronickému podepisování přidržet se definovaných standardů a zvýšila se tak kompatibilita mezi různými aplikacemi a tedy i jednoduchost používání.

3.5 Nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu

Na počátku dubna 2014 bylo přijato nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (zkráceně dále pouze Nařízení).

Od přijetí Směrnice se jedná patrně o jedno z nejzásadnějších opatření týkající se elektronického podpisu a kvalifikovaných poskytovatelů certifikačních služeb.

Vzhledem ke zvolené právní formě, bude Nařízení přímo aplikovatelné ve všech členských státech EU. V platnost vstoupí pravděpodobně 1. července 2014 (dvacátým dnem po zveřejnění v Úředním věstníku Evropské unie). Od tohoto data se zruší stávající směrnice 1999/93/ ES a odkazy na zrušenou směrnici budou považovány za odkazy na nařízení. Data účinnosti jednotlivých částí jsou s ohledem na nutnost předložení souvisejících prováděcích aktů a na potřebu přizpůsobení členských států odložena tak, že ustanovení nařízení budou nabývat účinnosti postupně podle přijetí prováděcích aktů v období 2015–2018 a povinnost vzájemně uznávat oznámené prostředky pro elektronickou identifikaci nabyde účinnosti v polovině roku 2018. Nařízení počítá s řadou přechodných opatření.[7]

Nařízení se dotkne zejména následujících oblastí[8]:

- důvěryhodná elektronická identita fyzické osoby,
- důvěryhodný podpis zaručující integritu a vazbu na identitu fyzické osoby,

[7,8] BÍLEK, Filip a Ondřej FELIX. Nařízení eIDAS: (nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu). In: Sborník konference ISSS 2014. s. 24 - 26.

- důvěryhodná značka zajišťující integritu a vazbu na právnickou osobu,
- důvěryhodné časové razítko zajišťující integritu a vazbu na čas,
- důvěryhodná služba registrovaného elektronického doručování zajišťující integritu a vazbu na odesílatele, adresáta a čas odeslání a doručení,
- důvěryhodný dokument se zaručenou integritou,
- důvěryhodnost webových stránek s vazbou na provozovatele.

Co se týče elektronického podpisu, Nařízení ze Směrnice 1999/93/ES vychází a rozšiřuje ji[9]:

Pojem „zaručený elektronický podpis“ (advanced electronic signature) zůstává zachován, ale nově se zavádí pojem „kvalifikovaný elektronický podpis“ (qualified electronic signature), který musí být založen na kvalifikovaném certifikátu a zároveň elektronický podpis musí být vytvořen pomocí kvalifikovaného zařízení pro vytváření elektronického podpisu (dnešní bezpečná zařízení pro tvorbu elektronického podpisu, tzv. SSCD zařízení, by měla být uznaná podle nového nařízení jako kvalifikovaná zařízení). Tento typ podpisu má mít stejné právní účinky jako vlastnoruční podpis ve všech členských státech, zatímco právní účinky u ostatních typů elektronických podpisů mají být definovány na úrovni národního práva.

[9] BÍLEK, Filip a Ondřej FELIX. Nařízení eIDAS

4 Právní úprava elektronického podpisu v ČR

Nejvýznamnějším právním předpisem v ČR, který se týká elektronického podpisu, je již zmíněný Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, který implementuje směrnici 1999/93/ES do českého právního řádu.

Dále je potřeba zmínit prováděcí vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, a vyhlášku č. 212/2012 Sb., o ověřování platnosti zaručeného elektronického podpisu.

Vyhláška č. 212/2012 Sb., o ověřování platnosti zaručeného elektronického podpisu, má dvě části, kde první se zabývá údaji, na základě kterých lze osobu jednoznačně identifikovat, a druhá se zabývá postupy pro ověřování zaručeného elektronického podpisu, elektronické značky a kvalifikovaného časového razítka.

5 Závěr

Tato práce měla za cíl popsat vývoj a současný stav legislativy EU týkající se elektronického podpisu, nastínit její pravděpodobný vývoj v blízké budoucnosti a zmínit způsob, jakým je příslušná evropská legislativa naplněna v českém právním řádu.

Úvodem práce byly popsány důvody, které vedou k masivní míře elektronické komunikace, která s sebou přináší i nové obchodní příležitosti a následně také změnu způsobu fungování orgánů veřejné moci ve vztahu k občanům. Čím dál více úředních podání, potvrzení nebo smluv je vyřizováno elektronicky a elektronický podpis je instrument, který byl díky svým specifickým vlastnostem, založeným na exaktních matematických metodách, legislativně upraven.

Po stručném nástinu principu fungování elektronického podpisu byly popsány podstatné právní předpisy EU týkající se elektronického podpisu, od prvotní Směrnice 1999/93/ES, přes rozhodnutí Komise, po zcela nové, právě schválené Nařízení, které Směrnici 1999/93/ES pravděpodobně již od 1. 7. 2014 nahradí.

Vzhledem k rozsahu práce byly pouze okrajově zmíněny právní předpisy ČR, které Směrnici 1999/93/ES v české legislativě implementují.

Problematika elektronického podpisu je však mnohem širší než bylo možné v této práci popsat. Záměrně vynechány byly pojednání o rozdílu mezi elektronickým podpisem, elektronickou značkou a časovým razítkem, což jsou všechno produkty stojící na principu, který byl vysvětlen v kapitole 3, nicméně jejich použití má různé právní důsledky. Ačkoliv byly tyto termíny zahrnuty již v Zákoně č. 227/2000 Sb. o elektronickém podpisu, ve Směrnici 1999/93/ES zmíněny nebyly a upravuje je až Nařízení, které teprve vstoupí v platnost a bude třeba čekat na prováděcí akty a přechodná opatření, které umožní novou legislativu detailně aplikovat v praxi. Rovněž témata jako požadavky na poskytovatele certifikačních služeb, ověřování elektronických podpisů nebo porovnání specifik lokálních legislativ souvisejících s elektronickým podepisováním jsou zajímavá a je možné uvažovat o rozšíření této práce dalšími směry.

Přesto se dle autora lze domnívat, že cíle definovaného v úvodu této práce bylo dosaženo.

6 Literatura

BÍLEK, Filip a Ondřej FELIX. Nařízení eIDAS: (nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu). In: Sborník konference ISSS 2014. s. 24 - 26. Dostupné z: http://www.isss.cz/archiv/2014/download/isss2014.pdf

BOSÁKOVÁ, Dagmar aj. Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů. 1.vyd. Olomouc: Anag, 2002, 141 s. ISBN 80-726-3125-X.

BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1.

Česká republika. Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů [online]. 2 s. [cit. 2012-03-13]. (PDF). Dostupné na WWW: <http://www.mvcr.cz/soubor/narizeni-vlady-c-495-2004-sb-kterym-se-provadi-zakon-c-227-2000-sb-o-elektronickem-podpisu-a-o-zmene-nekterych-dalsich-zakonu.aspx>.

Česká republika. Vyhláška č. 212/2012 Sb., o ověřování platnosti zaručeného elektronického podpisu [online]. 4 s. [cit. 2012-09-13]. (PDF). Dostupné na WWW: <http://www.mvcr.cz/clanek/vyhlaska-212-2012.aspx>.

Česká republika. Vyhláška č. 496/2004 Sb., o elektronických podatelnách [online]. 4 s. [cit. 2012-03-13]. (PDF). Dostupné na WWW: <http://www.mvcr.cz/soubor/vyhlaska-c-496-2004-sb-k-elektronickym-podatelnam.aspx>.

Česká republika. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) [online]. 24 s. [cit. 2012-03-15]. (PDF). Dostupné na WWW: <http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

Evropská unie. Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy ze dne 13. prosince 1999 [online]. 15 s. [cit. 2011-03-28].(PDF).Dostupné na WWW: <http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:CS:PDF>.

PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, c2011, 430 s. CZ.NIC. ISBN 978-80-904248-3-8.

The European Union. Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States [online]. 6 s. [cit. 2011-03-28]. (PDF). Dostupné na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF>.

The European Union. Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market [online]. 7 s. [cit. 2011-03-28]. (PDF). Dostupné na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF>.

The European Union. Corrigendum to Commission Decision 2009/767/ES of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the ‘points of single contact’ under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market [online]. 37 s. [cit. 2011-03-28]. (PDF). Dostupné na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF>.

Tománek, J. Problematika přeshraničního uznávání elektronických podpisů. (Diplomová práce) Praha: ČZÚ, 2011. 98 s.