UNIVERZITA KARLOVA

Právnická fakulta

Tereza Dvořáková

Elektronická identifikace osob v soukromoprávních poměrech

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Ondřej Frinta, Ph.D.

Katedra: Katedra občanského práva

Datum vypracování práce (uzavření rukopisu): 22. 6. 2018

Prohlášení autora

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 109 806 znaků včetně mezer.

Tereza Dvořáková

V Pardubicích dne 25. 6. 2018

Poděkování

Na tomto místě bych ráda upřímně poděkovala vedoucímu diplomové práce doc. JUDr. Ondřeji Frintovi, Ph.D. za veškerou poskytnutou pomoc, odborné vedení práce a velmi vstřícný přístup. Dále velice děkuji, a to nejen za poskytnuté odborné rady, Ing. Janu Kellerovi a Ing. Danielu Hromádkovi. Na závěr, avšak v neposlední řadě, děkuji z celého srdce své rodině, bez jejíž podpory, a to především té psychické, by tato práce nikdy nemohla vzniknout.

Obsah

Úvod

Tématem své diplomové práce jsem zvolila elektronickou identifikaci osob v soukromoprávních poměrech, a to z několika důvodů. Chtěla jsem vytvořit dílo, které bude svým způsobem určitým přínosem a nebude jen opakovaně řešit problematiku již mnohokrát rozebíranou. Vzhledem k tomu, že kontext elektronické identifikace je záležitostí postmoderní doby a všechny právní předpisy jí se zabývající jsou datovány zhruba v posledních dvou dekádách, zdála se tato oblast dostatečně otevřenou pro zisk nových poznatků.

Zároveň bych ve své práci chtěla přinést svým způsobem ucelený přehled institutů elektronické identifikace užívaných v soukromoprávních poměrech a vysvětlení jejich základních aspektů, aby čtenář nemusel při základním seznámení s problematikou hledat v mnoha normách nejen vnitrostátních, ale s ohledem na skutečnost, že se tyto instituty a jejich právní úprava podřizují v nemalé míre právu evropskému, i předpisech právě evropských, s nimiž je postupně český právní řád harmonizován. Tato diplomová práce by tedy měla vytvořit kompletní ucelený přehled elektronických identifikátorů používaných v soukromoprávních poměrech a vysvětlit jejich základní aspekty.

Dále by měl tento text osvětlit čtenáři historický vývoj a znázornit, jak se elektronická identifikace v posledních letech proměňovala a formovala do své současné podoby. Pochopení historických souvislostí z mé vlastní zkušenosti v mnohém usnadní následné pronikání do problematiky samotné a umožňuje lépe pochopit nejen samotné aspekty právních norem, ale v některých případech i záměr zákonodárce. Historie elektronických identifikátorů nesahá do minulosti nijak dávné, avšak právě díky tomu, že se tento vývoj udál až v posledních zhruba padesáti letech, je možné podrobnosti o něm získat z více zdrojů, je lépe zmapován a z důvodu úpravy aktuálních institutů je jeho chápání značně usnadněno. Ačkoliv kapitola o historii nástrojů elektronických identifikací není stěžejní nebo v porovnání s ostatními nejzásadnější, zařadila jsem ji jako úvodní, a to právě s ohledem na pozvolný úvod do řešené problematiky a poskytnutí kontextu, který může čtenáři pomoci se lépe orientovat nejen v kapitolách následujících, ale i v samotné oblasti jako takové. Věřím, že právě tento postup zajistí snadnou čitelnost a srozumitelnost práce. Domnívám se totiž, že pokud by tato kapitola v souboru chyběla, byla by cesta k pochopení a seznámení se s celou materií diplomové práce o poznání náročnější a prvotní setkání s ní by

pravděpodobně bylo zmatené a neuchopitelné. Cestu k dokonalému seznámení se s určitou problematikou skrze průchod od jejích počátků vnímám jako nejvhodnější a nejméně násilnou. Ostatně i výuka na naší fakultě, tedy Právnické fakultě Univerzity Karlovy, je započato tématy z historie vývoje právní vědy, ať už se jedná o nauku o právu římském, jež je pro soudobé soukromé právo velmi zásadním nebo české právní dějiny, které pomáhají pochopit zakotvení určitých aspektů z historických důvodů a jejich význam v současné legislativě. Myslím si, že kdybych si v prvním ročníku neprošla těmito kurzy a vyučující na mě v prvních dnech na vysoké škole vůbec začali chrlit právní terminologii a instituty soudobého práva bez alespoň základního úvodu do historie, byla by má cesta, kterou jsem prošla až do aktuálního, tedy pátého a závěrečného ročníku, podstatně náročnější.

Diplomová práce by také měla, navzdory skutečnosti, že je sepsána studentkou Právnické fakulty, poskytnout vysvětlení základních technologických aspektů elektronických identifikátorů. Ač nejsem odborníkem v kontextu informačních technologií, nebo možná právě proto, ráda bych čtenáři pomohla, alespoň v nezbytném rozsahu, pochopit, jak vlastně veškeré instrumenty, o nichž právní normy v obecné rovině hovoří, ve skutečnosti fungují. Samotnou mě tento aspekt celé věci od počátku zajímal, a proto jsem se rozhodla psaní diplomové práce využít též k získávání vlastních nových poznatků a rozšiřování obzorů. Protože sama bych se v naprosto neznámém odvětví velmi těžko začala orientovat a časová náročnost takového sebevzdělávání by byla nejen značná, ale vysoce pravděpodobně i neúnosná, dovolím si podotknout, že takto vynaložené úsilí by se dalo označit i za zbytečné, rozhodla jsem se využít znalostí přátel, kteří jsou v oboru informačních technologií profesionály. Doufám, že při dokončení své diplomové práce budu mít nejen o pár napsaných řádků ve svém portfoliu víc, ale budu mít i základní přehled v nové, dosud z mé strany téměř nedotčené problematice.

V neposlední řadě bych ráda rozebrala oblast elektronické identifikace v pouhé teoretické rovině, ale přenesla získané poznatky i do praxe. Právě s ohledem na to, jak moc je řešená oblast fenoménem pouhých několika málo posledních let, převažuje teorie a zakotvení v právních normách nad skutečným užíváním v běžném životě. Zvolila jsem řešení problematiky v soukromoprávních vztazích i proto, že se jedná o vztahy s především dispozitivní úpravou a velká část jejího uskutečňování je tedy na vůli subjektů. Ve vztazích s veřejnou mocí je fyzickým osobám poskytnuta i jakási míra jistoty vzhledem k presumpci, že orgány této moci jsou

s předmětnou oblastí seznámeny lépe, než běžní občané a vzhledem k užívání instrumentů během své každodenní činnosti získávají též tolik potřebné zkušenosti. Naproti tomu v poměrech mezi dvěma osobami soukromého práva se jedná ve většině případů o laiky na obou stranách a často především ze strachu z možného pochybení použijí tyto subjektu některou z více „zažitých" metod a spoléhají na jistotu v praxí ověřených postupech. Ráda bych tedy svou prací napomohla i k šíření povědomí o možnosti elektronické identifikace, která je metodou nejen časově i finančně méně náročnější, ale pro uživatele i bez dalších pochybností pohodlnější. Kromě toho spatřují výhodu opatřování dokumentů v elektronické podobě právě elektronickými identifikátory v tom, že je tato metoda dle mého názoru výrazně ekologičtější, kdy nevyžaduje opakované tisknutí listin v papírově podobě a jejich zasílání skrze poskytovatele poštovních služeb.

Doufám tedy, že se mi v následující práci podaří naplnit cíle výše vytyčené a tento soubor bude nejen pro odbornou, ale i laickou veřejnost přínosem. Věřím, že se mi podaří vytvořit text, který pomůže ke shrnutí rozebírané problematiky, vysvětlení jejích základních aspektů a vytvoření jasného a snadno uchopitelného přehledu. Každý čtenář by měl být po dočtení kompletní práce schopen si uvědomit a definovat základní aspekty elektronické identifikace, a to jak po stránce právní, tak po stránce technické, a kromě toho i umět popsané instrumenty aplikovat i v praxi. Práce se tedy může stát i jakýmsi návodem k základními použití pro ty, kteří se dosud s elektronickou identifikací v žádné formě nesetkali, ať už dílem náhody nebo se této záměrně ze strachu nebo jiných důvodů. Budu usilovat o to, aby se práce stala nejen textem užívaným především odbornou veřejností, kterým je samozřejmě v první řadě, ale částečně i dílem, které bude schopna uchopit i veřejnost širší.

1. Historický vývoj právní úpravy elektronické identifikace

Elektronická identifikace osob je bez jakýchkoli pochybností institutem výrazně moderním a novým. Tato oblast se počala výrazněji rozvíjet až vstupem do nového tisíciletí, a i do dnešního dne stále existuje v této oblasti jistá iluze zásadní odlišnosti a ve velké míře v ní figurují i obavy z důvěryhodnosti jednotlivých identifikátorů. Proto je nutné klást velký důraz na bezchybnou, co nejpodrobnější a podrobnou právní úpravu bez mezer, v níž nebude prostor pro odlišné výklady, případně i zneužití. Významným faktorem podporujícím důvěryhodnost elektronických podpisů a jim příbuzných institutů se též s postupem času stane judikatura. Výklad soudů přispěje v nezanedbatelné míře jistě i k upřesnění výkladu a sjednocení názorů na jednotlivá ustanovení právních předpisů zejména Evropské unie. Cesta vedoucí k ideální právní úpravě elektronické identifikace, která by umožnila kompletní nahrazení podpisů vlastnoručních, provedených na fyzicky existujících listinách, je tedy již do velké části prošlapaná, avšak stále ještě zbývá podstatný kus, který bude nutné v blízké době ještě ujít a posunout se tak opět blíže ke zjednodušení, zrychlení a zefektivnění další oblasti lidského života. V následující kapitole rozeberu historický vývoj, tedy tu část metaforické cesty, která již je, obrazně řečeno, za námi.

Počátek elektronických podpisů a elektronické identifikace vůbec sahají k době, kdy se začala objevovat a v praxi využívat tzv. asymetrická kryptografie, tedy způsob šifrování, který je pro tuto oblast zcela stěžejní. Jak jsem již naznačila v textu výše, jedná se o postup, při němž je jedinečný otisk dokumentu zašifrován soukromým klíčem odesílatele a k jeho dešifrování následně dochází po aplikaci veřejného klíče. V případě, že se otisky těchto dat shodují, je stvrzeno, že dokument nebyl při přenosu poškozen ani pozměněn.

První známou asymetrickou šifrou je šifra s veřejným klíčem RSA, která se poprvé objevila roku 1977. Do sedmdesátých let minulého století je tedy nejčastěji datován vznik asymetrické kryptografie. O necelých deset let později, roku 1985, navrhnul egyptský kryptograf Taher Elgamal nový algoritmus, nesoucí dodnes jeho jméno, tedy El-Gamal. Používání tohoto šifrování je však v dnešní době na ústupu, vzhledem k tomu, že jeho šifrovaná data objemem mnohonásobně převyšují data nešifrovaná, což je zásadním nedostatkem i například v porovnání s první uvedeným algoritmem. Pravděpodobně nejzásadnější šifrování pro oblast elektronické identifikace je DSA (z angl. zkratky Digital Signature Algorithm) vyvinutý americkým

institutem NIST roku 1991. Tento systém je užíván pouze pro elektronické podpisy a neumožňuje šifrování jiných dat. I přes svou striktní specifičnost je v oblasti elektronické identifikace v současnosti velmi hojně využíván.

Technologický pokrok v oblasti elektronické identifikace byl tedy v devadesátých letech minulého století již více než znatelný a taková situace nutně vyžadovala právní regulaci tohoto dynamického odvětví.

1.1. Vývoj evropské právní úpravy

Průkopníkem v oblasti elektronické identifikace bylo v evropském kontextu Německo. Tamní zákon o elektronickém podpisu (Gesetz zur digitalen Signatur vom 22. Juli 1997) pochází již z 22. července 1997 a je doplněn Vyhláškou k elektronickému podpisu (Verordnung zur digitalen Signatur vom 22. Oktober 1997) z 22. října roku téhož. Stejně překvapivě rychle došlo u našich západních sousedů i k aktualizaci právní úpravy danou problematikou se zabývající. První normy z roku 1997 byly nahrazeny novou regulací už 22. května 2001, kdy nabyl účinnosti zákon o rámcových podmínkách pro elektronický podpis (Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001) opět doplněný Vyhláškou k elektronickému podpisu (Verordnung zur elektronischen Signatur vom 16. November 2001). Nová právní úprava byla v Německu přijata z důvodu harmonizace evropského práva, a to v reakci na vydání Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (dále jen „Směrnice 1999/93/ES“). Nejednalo se však o žádné zásadní změny v této oblasti, nový německý zákon o elektronickém podpisu se v mnohém shodoval se svým předchůdcem, avšak jeho přijetí bylo pro účely co nejdokonalejší harmonizace evropských právních systémů žádané. Nejenom četnost právních podkladů pro oblast elektronické identifikace, ale i rychlost, s níž spolková země na rychle postupující technologický pokrok v této oblasti reagovala, je příkladná. [1]

[1] HARTL, Jan. Srovnání legislativy elektronického podpisu v ČR a v Německu. Praha, 2006. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce doc. Ing. Prokop Toman, CSc., [cit. 13. 6. 2018].

1.1.1. Směrnice o zásadách Společenství pro elektronické podpisy

Směrnice 1999/93/ES byla stěžejním a průlomovým pramenem práva v oblasti elektronické identifikace v evropském kontextu. Jednalo se o první ucelenou právní úpravu této relativně nové a dynamicky se rozvíjející oblasti, která stanovovala závazná pravidla pro státy Evropské unie a stala se vzorem pro tvorbu pravidel vnitrostátních, která se na přelomu tisíciletí povětšinou nenacházela na té nejvyšší úrovni a pravidla harmonizace v tomto období neznamenala natolik přítěž, jako spíše vodítko a poskytnutí funkčního vzoru.

Podnětem k sepsání Směrnice 1999/93/ES bylo sdělení Evropské komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů o evropské iniciativě v oblasti elektronického obchodu ze dne 16. dubna 1997. Následně dne 1. prosince 1997 Rada vyzvala Komisi, aby co nejdříve předložila návrh směrnice Evropského parlamentu a Rady o digitálních podpisech. Jejím účelem mělo být zejména odstranit rozdíly v předpisech členských států o uznávání elektronických podpisů v rámci elektronické komunikace a obchodu, které by mohly v případě absence této regulace narušit volný pohyb v rámci vnitřního trhu Evropské unie a narušit důvěryhodnost nových technologií a jejich následného uznávání.

Dalšími účely, které měla směrnice naplnit bylo například nalezení rovnováhy mezi potřebami spotřebitelů a podniků, umožnění poskytování ověřovacích služeb jak veřejnoprávními jednotkami, tak i fyzickými či právnickými osobami a zabránění omezování hospodářské soutěže v odvětví ověřovacích služeb akreditačními systémy.

Směrnice tyto požadavky naplňující byla spolu se čtyřmi přílohami, specifikující požadavky na kvalifikovaná osvědčení, ověřovatele tyto kvalifikovaná osvědčení vydávající, požadavky na prostředky pro bezpečné vytváření elektronických podpisů a doporučení pro bezpečné ověřování podpisu představena dne 13. 12. 1999. Lhůta pro harmonizaci vnitrostátních předpisů byla členským státům stanovena do 19. července 2001.

Zajištění dohledu nad dodržováním směrnice a způsob jeho provedení byl ponechán na vůli jednotlivých členským státům Unie, stejně tak jako proces harmonizace s vnitrostátním právem. Výslovně stanovuje, že nevylučuje vytvoření

systému dohledu v soukromém sektoru a neukládá ověřovatelům povinnost žádat o výkon dohledu v rámci jakéhokoli platného akreditačního systému.

Směrnice 1999/93/ES byla zrušena nařízením eIDAS, jak je na první pohled zřejmé z koncové části jeho názvu (tedy: o zrušení směrnice 1999/93/ES), a to z důvodu, že neposkytovala ucelený přeshraniční a meziodvětvový rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce. Jednalo se pouze o omezenou úpravu elektronických podpisů jako takových. Nařízení eIDAS mělo přispět k vytvoření jednotného digitálního trhu vytvořením vhodných podmínek pro vzájemné uznávání klíčových prvků mezi jednotlivými členskými státy. Dále bylo zajisté nutné reagovat na rychlý technologický rozvoj v oblasti elektronických podpisů, nebylo udržitelné aplikovat stejné právní předpisy, které striktně reflektují technologické aspekty dané problematiky, jako před téměř dvaceti lety. Nařízení eIDAS se tedy stalo novou, modernější a komplexnější úpravou elektronické identifikace, která odpovídá požadavkům dvacátých let 21. století a její použitelnost je značně široká.

1.2. Vývoj vnitrostátní právní úpravy

Vnitrostátní právní úprava byla v evropském kontextu spíše opožděná. První ucelenější právní úpravou elektronických podpisů se stal právě až ZEP, kromě samotné normy jako takové byly učiněny pouze dílčí zásahy do stávajících předpisů, v nichž bylo nutné nastupující trend elektronické identifikace reflektovat (např. zákon č. 40/1994 Sb., občanský zákoník, zákon č. 99/1963 Sb., občanský soudní řád nebo zákon č. 337/1992 Sb., o správě daní a poplatků).

1.2.1 Zákon o elektronickém podpisu

ZEP se stal prováděcím zákonem pro Směrnici 1999/93/ES na území České republiky. Platnosti nabyl 26. 7. 2000, účinnosti potom v souladu s § 28 prvním dnem třetího kalendářního měsíce po dni jeho vyhlášení, tedy 1. 10. 2000. Česká republika tedy dodržela lhůtu stanovenou pro harmonizaci právního řádu s evropskou úpravu s dostatečnou rezervou. ZEP nebyl v žádném případě rozsáhlou právní normou, včetně společných a změnových ustanovení a ustanovení o jeho účinnosti byl tvořen v celku pouhými 28 paragrafy.

ZEP navzdory svému názvu neupravoval jen problematiku elektronických podpisů jako takových, ale byly v něm vymezeny všechny základní druhy elektronické identifikace, tedy primárně podtypy samotných elektronických podpisů – běžný, zaručený, zaručený založený na kvalifikovaném certifikátu, uznávaný a na závěr i elektronické značky.

Jedním z nejstěžejnějších byl bezesporu druhý paragraf ZEP, který vymezil základní pojmy v normě užívané. Vzhledem ke skutečnosti, že se jednalo o problematiku novou a dosud upravenou pouze roztříštěně a útržkovitě, pokud nevyužijeme odkazu na úpravu evropskou, seznámení s terminologií bylo elementární.

V následujících ustanoveních jsou specifikovány požadavky na soulad dat, povinnosti podepisujících a označujících osob, držitelů certifikátu, poskytovatelů, podmínky a náležitosti jednotlivých forem elektronické identifikace a jejich zrušení. K dalšímu významnému ustanovení se dostáváme s § 16, jenž upravuje uznávání zahraničních kvalifikovaných certifikátů, a to především v rámci Evropské unie. V tomto ustanovení je tedy harmonizace s evropským právem nejznatelnější a projevuje se povaha ZEP jako prováděcího zákona pro Směrnici 1999/93/ES. Následuje úprava prostředků pro vytváření a ověřování elektronických podpisů a značek, správních deliktů a přestupků, společná a zmocňovací ustanovení. Na závěr celé normy jsou upraveny změny konkrétních souvisejících právních norem, jako například zákona č. 99/1963 Sb., občanský soudní řád, zákona č. 141/1961 Sb., trestní řád, zákona č. 101/2000 Sb., o ochraně osobních údajů a zákona č. 368/1992 Sb., o správních poplatcích. Posledním paragrafem je výše zmíněný § 28 stanovující účinnost ZEP na první den třetího kalendářního měsíce po dni jeho vyhlášení.

2. Typy elektronické identifikace v soukromém právu

Pro účely seznámení se základními typy elektronické identifikace osob v soukromém právu je v první řadě bezpodmínečně nutné vymezit oblast soukromého práva jako takovou. Dualismus práva soukromého a veřejného je jedním ze základních problémů, jimiž se právní věda zabývá. V minulosti byla vytvořena celá řada teorií, podle nichž měly být tyto dvě oblasti rozlišovány.

První z výše zmíněných teorií prosazoval římský právní vědec Domitius Ulpianus a je označována jako teorie zájmová. Toto pojetí je zachyceno v Digestech následující větou: „*Publicum ius est quod ad statum rei Romanae spectat, privatum quod ad singulorum utilitatem*.“, tedy v překladu: „*veřejné právo je to, které se týká postavení římského státu, soukromé které se vztahuje k prospěchu jednotlivců*“[2]. Dle tohoto výkladu lze rozeznat právo soukromé a veřejné právě podle zájmu, k jejichž ochraně má daná oblast práva směřovat. Zatímco první zmíněné, tedy právo soukromé, chrání především zájmy jednotlivce, právo veřejné v protikladu poskytuje ochranu zájmům celospolečenským.

Druhou metodou je rozdělení dle tzv. teorie mocenské neboli subordinační, jež je založena na vzájemném postavení, tedy vztahu vzájemné podřazenosti a nadřazenosti subjektů daného práva. Zatímco v soukromoprávní sféře je preferován princip vzájemné rovnosti a nemožnosti autoritativně určovat práva nebo povinnosti zúčastněných subjektů, na druhé straně v poměrech veřejnoprávních je typicky jeden ze subjektů v postavení nadřazeném vůči subjektům ostatním a je oprávněn tyto jednostranně zavazovat. K mocenské teorii se v minulosti přiklonila i judikatura Ústavního soudu České republiky, když vymezila veřejnou moc následujícím způsobem: „*veřejnou mocí se rozumí taková moc, která autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo, nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není v rovnoprávném postavení s tímto orgánem a obsah rozhodnutí tohoto orgánu nezávisí od vůle subjektu*“[3]. Navzdory tomu je nutné připustit,

[2] Digesta, neboli, Pandekty: svazek I, kniha I-XV, vybrané části = Digesta, seu, Pandecta: tomus I, liber I-XV, fragmenta selecta. Přeložil Peter BLAHO, přeložil Jarmila BARTOŠÍKOVÁ, přeložil Michal SKŘEJPEK, přeložil Jakub ŽYTEK. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. Fontes iuris romani, str. 125.

[3] Nález Ústavního soudu ze dne 1. 12. 1998, sp. zn. I. ÚS 41/98 (N 147/12 SbNU 363) s odkazem na usnesení Ústavního soudu ze dne 25. 11. 1993, sp. zn. II. ÚS 75/93 (U 3/2 SbNU 201).

že i toto pojetí má několik podstatných nedostatků, vzhledem ke skutečnosti, že i v rámci soukromého práva existují instituty, kde si jsou zúčastněné subjekty rovny (typicky například veřejnoprávní smlouvy) a naopak vztah rovnosti v soukromoprávních poměrech nemusí být stoprocentně dodržen kupříkladu u smluv uzavíraných se spotřebitelem, kdy je spotřebitelovo postavení výrazně zvýhodněno.

Trojici nejvýznamnějších teorií dualismu soukromého a veřejného práva uzavírá tzv. teorie organická, která je v současnosti i nejčastěji používána. Ta vymezuje jako veřejnoprávní vztahy takové, v nichž je jeden ze subjektů orgánem veřejné moci. Všechny zbylé poměry považuje za poměry soukromoprávní[4].

Ačkoliv o jasné rozlišení pojmů práva soukromého a veřejného právní věda usiluje již od svého prvopočátku, ani v současnosti není toto rozlišení zcela zřetelné a hranice jejich dualismu ostře vymezené. I v současné době existují nejen konkrétní instituty, ale i celá právní odvětví (jako např. právo pracovní), jejichž zařazení do konkrétního subsystému není zcela jednoznačné a mohou obsahovat jednotlivé prvky obou z nich.

Pro účely mé práce budu vycházet zejména z teorie organické, vyloučím tedy jako veřejnoprávní veškeré vztahy, ve kterých vystupuje jako jeden z účastníků orgán veřejné moci. Dále budu za soukromoprávní považovat ty vztahy, jež jsou založeny na autonomii vůle a s tím související dispozitivní právní úpravou, jak ostatně stanovuje i § 1 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „OZ“).

V soukromoprávních poměrech se tedy používají především dva základní a jeden doplňkový typ elektronické identifikace osob. Stěžejními jsou elektronický podpis uznávaný a elektronický podpis prostý. Tyto dva druhy vymezuje zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění (dále jen „ZSVDET“). Třetím typem je potom dynamický biometrický podpis, který není dosud stávající právní úpravou zohledněn, avšak je výkladovou praxí jako platný přijímán.

Pro doplnění bych dále zmínila, že ve vztazích veřejnoprávních se používají jako prostředky elektronické identifikace osob kvalifikovaný elektronický podpis, kvalifikovaná elektronická pečeť a elektronické časové razítko. První z výše zmíněných upravuje § 5 ZSVDET, který stanoví povinnost použít kvalifikovaný elektronický

[4] GERLOCH, Aleš. Teorie práva. 7. aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. Právnické učebnice (Aleš Čeněk), str. 126.

podpis při podpisu dokumentů, jimiž právně jedná stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem. Pro tyto subjekty zákon vytváří legislativní zkratku a dále je označuje jako veřejnoprávní podepisující. Kromě veřejnoprávních podepisujících použije kvalifikovaný elektronický podpis i jiná osoba při výkonu své působnosti v oblasti veřejné správy. Vzhledem k přechodným ustanovením, konkrétně § 19 odst. 1 ZSVDET je však veřejnoprávním podepisujícím po dobu dvou let od účinnosti tohoto zákona, tedy do 19. 9. 2018 umožněno učinit výběr, zda použít kvalifikovaného elektronického podpisu nebo připojit k listině zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis. Takovým podpisem rozumíme dle § 6 odst. 2 ZSVDET uznávaný elektronický podpis, o kterém bude pojednávat další část mé práce.

Co se týče elektronických pečetí, jedná se prostředek, který slouží k označení a prokázání původu a pravosti konkrétního dokumentu. Ustanovení § 8 ZSVDET uděluje veřejnoprávním podepisujícím povinnost zapečetit dokument v elektronické podobě kvalifikovanou elektronickou pečetí pro případy, v nichž nestanoví jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání. Tato povinnost je, stejně jako u kvalifikovaných elektronických podpisů, přechodným ustanovením v § 19 odst. 2 odložena a přechodné období končí též 19. 9. 2018. Do tohoto data mohou veřejnoprávní podepisující zaručenou elektronickou pečeť založenou na certifikátu pro elektronickou pečeť vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru nebo elektronickou značku podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, v platném znění (dále jen „ZEP“). Tento zákon byl sice k 18. 9. 2016 zrušen, avšak právě výše zmíněné ustanovení ZSVDET prodlužuje životnost elektronických značek o přechodné dvouleté období. Výhodou elektronických pečetí oproti elektronickým značkám je možnost použití a uznání v rámci celé Evropské unie, kterou zajišťuje zakotvení institutu v nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „eIDAS“). Dosavadně používané elektronické značky byly pouze českým specifikem a v okamžiku, kdy jimi opatřený dokument opustil území České republiky, přestala elektronická značka okamžitě plnit

požadovanou funkci, tedy prokázání nejen integrity, ale i důvěryhodnosti daného, jí opatřeného, dokumentu.

Posledním typem elektronické identifikace, který se ve veřejném právu objevuje, je potom kvalifikované elektronické časové razítko. Elektronické časové razítko dokládá existenci dokumentu v čase, tedy slovy výkladových ustanovení nařízení eIDAS se jedná o data v elektronické podobě, která prokazují, že určitý dokument v daném okamžiku existoval a spojuje tedy tento dokument s určitým časovým okamžikem. Použití elektronického časového razítka specifikuje § 11 ZSVDET, dle něhož každý veřejnoprávní podepisující, který podepsal elektronický dokument podle § 5 téhož zákona a osoba, která učinila stejně při výkonu své působnosti, musí takto podepsaný dokument opatřit elektronickým časovým razítkem. Stejně tak musí kvalifikované elektronické časové razítko tyto subjekty i k dokumentům, které zapečetily elektronickou pečetí.

Co se týče aktuálního stavu právní úpravy, dala by se označit za částečně svým způsobem předběžnou. Podle mého názoru nakládali zákonodárci s instituty, jejichž fungování a praktická aplikace nebyly ještě v té době na takové úrovni, aby bylo možné o těchto nástrojích vytvořit dokonalou, přehlednou a všeobsahující legislativu. Otázkou zůstává, zda vůbec některý z předpisů může takovéto požadavky splňovat, avšak pokud je odpověď na tuto otázku záporná, nutno podotknout, že kvalitní předpisy, které pracují s již známými fakty, poměry a instituty, se této definici více přibližují. Hlavním nedostatkem je z mého pohledu především chybějící právní úprava dynamických biometrických podpisů. Tento typ se dá sice zahrnout pod definici, jimž legislativa vymezuje elektronické podpisy, takže se o takový nástroj bez dalších pochybností jedná, avšak vzhledem k tomu, že nesplňuje náležitosti žádné z „vyšších“ forem elektronických podpisů, jedná se o pouhý elektronický podpis prostý. Tato skutečnost je však zcela absurdní. Při učinění takového zhodnocení jsem vyšla především z faktu, že jsem se při psaní této práce pokusila dostat blíže k pochopení dynamických biometrických podpisů a samotnou mě překvapilo, kolik dat o podepisujícím je možné z většinou jedné linky, jejíž vytvoření trvá několik málo vteřin, ve výsledku zjistit. Nad to jsem zjistila, že i tento typ podpisu je ať už ve specializovaném zařízení nebo za použití vhodného programu okamžitě šifrován a původní nechráněná data jsou ze všech systémů ihned po dokončení procesu šifrování vymazána. V tomto ohledu je naprosto nepochopitelné, že takto získaná data mají podle platné legislativy stejnou hodnotu, jako například oskenovaný vlastnoruční podpis

nebo PIN kód zadaný do klávesnice, případně pouhá patička v elektronické poště nebo odškrtnutí políčka na webové stránce. Ve skutečnosti a běžné praxi je samozřejmě dynamický biometrický podpis oceňovaný jako vyšší forma, někdy dokonce upřednostňovaný před podpisem vlastnoruční, z něhož vlastně nic jiného, než grafickou podobu jména podepisujícího není možné zjistit, avšak tento postup nemá žádný zákonný podklad. Pevně věřím, že na tento stav brzy zákonodárci zareagují a bude provedeno přehodnocení vymezení forem elektronických podpisů, jejich detailnější vymezení a rozdělení konkrétních technologií pod jednotlivé nadřazené pojmy.

2.1. Elektronický podpis

Elektronickým podpisem se podle nařízení eIDAS rozumí: „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání*“[5]. Tato definice je na první pohled velmi obecná, avšak tato obecnost je pravděpodobně na místě, vzhledem k tomu, že se jedná o novou právní úpravu, která by měla upravovat nejen elektronické podpisy, jak je znal původní ZEP, ale i další formy, které se na základě stále rychleji postupujícího technického pokroku během posledních let objevily, jako je například podpis biometrický, jímž se budu zabývat dále v této kapitole. Podrobnější vymezení těchto jednotlivých typů elektronické identifikace přinese až judikatura. Ta by mohla postupem času vyloučit z této definice např. pouhý podpis v e-mailu, který dosud při použití jazykového výkladu tomuto vymezení stále odpovídá. K vytvoření podpisu, který odpovídá tomu vlastnoručnímu, tedy postačí pouze na závěr e-mailu stejným způsobem jako jeho text napsat i vlastní identifikační údaje, případně připojit oskenovaný podpis a předcházející text se považuje za podepsaný se stejnými důsledky jako by se jednalo o dopis podepsaný vlastnoručně.[6]

Co se týče uznávání právních účinků elektronických podpisů obecně, je nejdůležitějším předpisem v této oblasti beze sporu čl. 25 eIDAS, který obsahuje

[5] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

[6] Kdy je nově prostý elektronický podpis rovnocenný s podpisem vlastnoručním?. Epravo [online]. 2017, 12. 1. 2017 [cit. 2018-03-18]. Dostupné z: https://www.epravo.cz/top/clanky/kdy-je-nove-prosty-elektronicky-podpis-rovnocenny-s-podpisem-vlastnorucnim-104697.html.

poměrně zásadní odstavec č. 1, v němž je stanoveno: „*Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy*“.[7] Pojem kvalifikovaného elektronického podpisu jsem rozebírala již výše a vzhledem ke skutečnosti, že se jedná o instrument používaný ve stycích veřejnoprávních, tedy nespadající pod rozsah této práce, nebudu v tuto chvíli tento rozbor dále rozšiřovat.

2.1.1. Elektronický podpis uznávaný

První z typů elektronických podpisů užívaných v soukromoprávním styku je uznávaný elektronický podpis, jež ZSVDET ve svém § 6 odst. 2 definuje jako: „*zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis*“. V této definici lze spatřit zásadní odlišnost od původního ZEP, který podpis zaručený a uznávaný považoval za dva odlišné typy. Uznávaný podpis stvrzoval podle staré právní úpravy identitu podepisující osoby, zatímco podpis zajištěný zaručoval pouze integritu dokumentu, tedy její nezměnění po okamžiku, v němž byl podpis připojen. Pro akceptaci uznávaných elektronických podpisů též není třeba, aby certifikát podpisu obsahoval upřesňující identifikátor podepisující osoby typu identifikátoru klienta Ministerstva práce a sociálních věcí (dále jen „MPSV“)[8].

Co se týče použití uznávaných podpisů, ZSVDET jej v § 6 odst. 1 přímo vyžaduje při podpisu elektronického dokumentu, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti. Uznávaný elektronický podpis může být též v přechodném období dvou let po nabytí účinnosti ZSVDET použit v situacích, které by za standardních podmínek vyžadovaly připojení kvalifikovaného elektronického podpisu, jak jsem již uvedla výše. V některých případech, v nichž se použije uznávaný podpis je tedy zřejmý prvek veřejnoprávní a při aplikaci organické teorie, jejíž použití jsem pro tuto práci již výše stanovila, se bude jednat o poměr veřejnoprávní. Podle mého uvážení se však jedná

[7] Čl. 25 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
[8] DONÁT, Josef. Nařízení eIDAS: komentář. Praha: C. H. Beck, 2017. Beckovy komentáře.

pouze o určitou část praktického využití uznávaného elektronického podpisu a není tedy vyloučeno, že se může jednat též o instrument, který bude využit v poměru soukromoprávním. Z tohoto důvodu jsem i tento typ zařadila do své práce a budu se jim zabývat více a podrobněji než nástroji, které při podpisu dokumentů musí nutně použít veřejnoprávní podepisující a tento prvek je zde tedy vysoce pravděpodobně nevyhnutelný. Tyto typy elektronických identifikátorů jsem tedy ze souboru vyřadila a jsou zde zmíněny pouze okrajově.

Aby mohl být uznávaný elektronický podpis v praxi používán, musí obligatorně splnit náležitosti vymezené v čl. 26 nařízení eIDAS, který specifikuje požadavky na zaručené elektronické podpisy. Ty musí být v první řadě jednoznačně spojeny s podepisující osobou, umožnit její identifikaci (v tomto bodě dochází k rozšíření původní právní úpravy, konkrétně směrnice č. 1999/93 o zásadách společenství pro elektronické podpisy a jejího čl. 2 odst. 2, která stanovovala pouze povinnost umožnit zjištění totožnosti podepisující osoby), dále musí zaručený podpis vzniknout pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou a na závěr musí být zaručené elektronické podpisy k datům, která jsou tímto způsobem podepsána, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Ve druhé části výše uvedené definice uznávaných elektronických podpisů je zmíněno jejich založení na kvalifikovaném certifikátu pro elektronický podpis. Co si však pod tímto kvalifikovaným certifikátem máme představit? Poměrně detailní definici tohoto pojmu nabízí čl. 28 nařízení eIDAS, následně s odkazem na jeho Přílohu 1. Podle tohoto vymezení musí každý kvalifikovaný certifikát pro elektronické podpisy obsahovat v první řadě označení, že byl daný certifikát vydán jako kvalifikovaný certifikát pro elektronické podpisy, dále potom soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, přičemž tímto poskytovatelem rozumíme takovou fyzickou či právnickou osobu, která poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele. Orgán dohledu musí být určen každým členským státem, který mu zároveň udělí i nezbytné pravomoci a odpovídající zdroje pro plnění jejich úkolů. Každý takový orgán musí do 31. března vždy předložit Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce, a to spolu shrnutím oznámení o narušení bezpečnosti, která obdrží od poskytovatelů služeb vytvářejících důvěru. V České republice je takovým orgánem Ministerstvo vnitra (dále jen „MV“).

Vrátím-li se zpět k podstatným náležitostem kvalifikovaného certifikátu pro elektronické podpisy, třetím požadavkem, který je nutno splnit, je jméno podepisující osoby nebo pseudonym, pokud si však podepisující osoba zvolí použití pseudonymu, tato skutečnost musí být jasně vyznačena. Dalším nutným aspektem jsou potom zcela přirozeně data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro jejich vytváření, označení začátku a konce doby platnosti předmětného certifikátu, identifikační číslo certifikátu (jedinečný údaj spojený s daným kvalifikovaným poskytovatelem služeb vytvářejících důvěru), dále musí být kvalifikovaný poskytovatel služeb vytvářející důvěru vydávající certifikát jednoznačně identifikován svým zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí, a dále potom údaje o místu, na němž je k dispozici certifikát, na kterém je předmětný zaručený elektronický podpis či zaručená elektronická pečeť založena. Dalšími údaji, které musí být součástí kvalifikovaného certifikátu pro elektronické podpisy, jsou potom údaje o umístění služeb, které lze využít k zjištění platnosti certifikátu a posledním požadavkem je potom v případě, že jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku o této skutečnosti. Taková poznámky musí být přiložena alespoň ve formě vhodné pro automatické zpracování, stejně tak jako první výše zmíněný požadavek, tedy označení, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis.

Dalším ustanovením nařízení eIDAS, které se váže k uznávaným elektronickým podpisům je potom jeho článek 25. V jeho druhém odstavci je stanoveno, že právní účinek rovnocenný vlastnoručnímu podpisu má kvalifikovaný elektronický podpis. Podle přechodných ustanovení v § 19 ZSVDET je možné používat uznávaný elektronický podpis obdobně, jako elektronický podpis kvalifikovaný, jak tedy vyplývá z výkladu těchto dvou ustanovení a jak zároveň shrnuje i komentář k nařízení eIDAS, v období do 19. 9. 2018 je možné přisuzovat uznávanému elektronickému podpisu právní účinky podpisu vlastnoručního. Na doplnění uvádím, že podle důvodové zprávy k nařízení eIDAS článek 25 objasňuje a rozšiřuje článek 5 směrnice 1999/93/ES zavedením výslovné povinnosti přiznávat kvalifikovaným elektronickým podpisům, potažmo tedy elektronickým podpisům uznávaným, stejný právní účinek jako vlastnoručním podpisům. Toto ustanovení je však částí odborné veřejnosti přijímáno při nejmenším s rozpaky, a to z toho důvodu, že by se dalo

předpokládat a očekávat postavení uznávaného elektronického podpisu minimálně na roveň podpisu úředně ověřenému, nikoli pouze vlastnoručnímu.

2.1.2. Elektronický podpis prostý

Takzvaný prostý elektronický podpis není zákonem vymezen zcela konkrétně. Poněkud vágní definici můžeme nalézt v § 7 ZSVDET, který hovoří o tom, že je možné použít: „*zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1*“. Právě tento „jiný typ elektronického podpisu“ zahrnuje tuto „zbytkovou“ kategorii, tedy elektronický podpis prostý, který se použije v situacích, kdy se stvrzuje právní jednání dvou soukromoprávních osob a není nutné užití některých přísnějších, podrobněji upravených forem elektronické identifikace. V takových poměrech pak prostý elektronický podpis tvoří adekvátní náhradu podpisu vlastnoručního.

Označení „prostý“ ZSVDET sám nepoužívá, bylo vytvořeno až praxí a zahrnuje tedy veškeré další druhy elektronických podpisů, kromě podpisů kvalifikovaných a uznávaných, v zákoně označené jako „jiný typ elektronického podpisu“.

Jako prostý elektronický podpis je možné chápat dosud právní naukou identifikovaných devět možných institutů.[9] Prvním z těchto je napsání jména v e-mailu. Ač se tento úkon může zdát na ověření identifikace dané osoby v současnosti poněkud nedostačujícím, všechny požadavky kladené na prostý elektronický podpis splňuje, a proto pouhé „vytypování“ vlastního jména na závěr e-mailu vytvoří právní domněnku opatření tohoto dokumentu právě prostým elektronickým podpisem. A co více, pokud se u odeslaného e-mailu zobrazuje adresa odesílatele, lze již tuto považovat za ona zákonem vymezená „data v elektronické podobě, jež jsou logicky spojena s jinými daty v elektronické podobě“ a zařadit tedy tuto jako další typ právně relevantního elektronického podpisu. Podobným způsobem lze prostý elektronický podpis připojit i k jinému elektronickému dokumentu, tedy například takovému, jež byl vytvořen v textovém editoru. Čtvrtým typem technické implementace elektronického podpisu

[9] S. Mason: Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation, In: SCRIPTed [online], 2012, 9:1, str. 82-103, str. 84, cit. [22. 4. 2018]. Dostupné na <http://script-ed.org/?p=327>.

v jeho nejjednodušší formě je potom zadání kódu PIN. Tento úkon představuje potvrzení přechozího jednání určitého subjektu zadáním unikátního číselného kódu a je způsobilé naplnit požadované podmínky. Dalším způsobem, který představuje stvrzení určitého konání připojením prostého elektronického podpisu je potom tzv. „click wrap method“, jak ji ve svém díle označuje Stephen Mason, britský advokát a jeden z největších expertů na problematiku elektronických podpisů a elektronické identifikace všeobecně. Tato metoda znamená ve skutečnosti pouhé prosté „kliknutí“ na možnost „I accept“ případně „I agree“ nebo poté v češtině „Souhlasím“ při pohybu v elektronickém prostředí, ať už při udělení souhlasu se zpracováním osobních údajů nebo při nakupování on-line. Tato možnost přitom bezpodmínečně nevyžaduje vyplnění osobních údajů před potvrzením. V některých případech však jejich poskytnutí bude nutné, jako je tomu například při on-line nákupu letenek. Při tomto postupu jsou osobní údaje kupujícího natolik stěžejními a významnými, že prodávající aerolinky dokonce provádí několikanásobné ověřování a srovnávání s existujícími databázemi. Toto ověření se děje, dá se říci v pozadí a zákazník o něm nemusí mít nejmenší ponětí. Zajistí však naplnění stále se zvyšujících požadavků na bezpečnost při cestování zejména v letecké dopravě. [10]

Velmi často řešenou problematiku představuje skenování vlastnoručních podpisů. V praxi je opakovaně rozebíraná otázka, zda může jako prostý elektronický podpis sloužit jednak přidání oskenovaného vlastnoručního podpisu k elektronickému dokumentu a v souvislosti s tím oskenované listiny, na jejímž konci je vlastnoruční podpis připojen. Všeobecně převládajícím je potom názor, že obě dvě tyto formy jsou způsobilé vlastnoruční podpis adekvátně zastoupit. Jedním z hlavních důvodů pro uznání oskenovaných podpisů jako prostých elektronických je potom jejich povaha, kterou se dají poměrně těsně srovnat s dnes již pouze zřídka používanou metodou faxování. Stejně, jako byla dříve vlastnoručně podepsaná listina odeslána k příjemci faxem, v dnešní době umožňuje ušetřit čas i finanční prostředky, jež by bylo nutné vynaložit na zaslání ve fyzické podobě prostřednictvím poskytovatele poštovních služeb nebo případně osobní předání dokumentu, je v dnešní době možné jej

[10] MGR. ING. KMENT, Vojtěch. NAHRADÍ ELEKTRONICKÝ PODPIS PROSTÝ TEN TRADIČNÍ VLASTNORUČNÍ?. Bulletin advokacie [online]. 2016, 2016 [cit. 2018-06-10]. Dostupné z: http://www.bulletin-advokacie.cz/nahradi-elektronicky-podpis-prosty-ten-tradicni-vlastnorucni?browser=full

opatřit skenem vlastnoručního podpisu, případně po vytištění oskenovat celou listinu, k níž byl vlastnoruční podpis připojen a následně zaslat prostřednictvím elektronické pošty.

Na závěr zmíním pravděpodobně technologicky nejnáročnější a nejkomplikovanější formy, v nichž je možné prosté elektronické podpisy užívat, a to konkrétně dynamický biometrický podpis a podpis digitální. K prvnímu zmíněnému typu se vrátím v následujících kapitolách své práce, vzhledem k tomu, že je dnes velmi často v praxi využívaným a částečně problematickým institutem. Co se týče podpisu digitálního, jedná se o formu, která je velmi často zaměňována s pojmem, jež je mu výrazně nadřazen, a to přímo elektronický podpis. V praxi se, zejména z důvodu nepřesných překladů velmi často pojem elektronického a digitálního podpisu vůbec neodlišuje. Jedná se však o velmi závažnou chybu, vzhledem ke skutečnosti, že digitální podpis je pouze jednou z možných forem podpisu elektronického. Význam druhého zmíněného pojmu je tedy výrazně širší a podřazuje pod sebe několik dalších prostředků, mezi nimi i právě podpis digitálním. Digitálním podpisem, pro přesnost je zde možná na místě uvést dovětek „v užším slova smyslu“ je tedy prostředek, jež za použití asymetrické kryptografie umožňuje podepsat dokument unikátním privátním klíčem, jímž disponuje pouze podepisující. Ověření je následně možné klíčem veřejným, kterým podepisující daný dokument následně opatří. Pro názornost a usnadnění pochopení této poměrně složité konstrukce připojuji schematický nákres (Obrázek 1)[11].

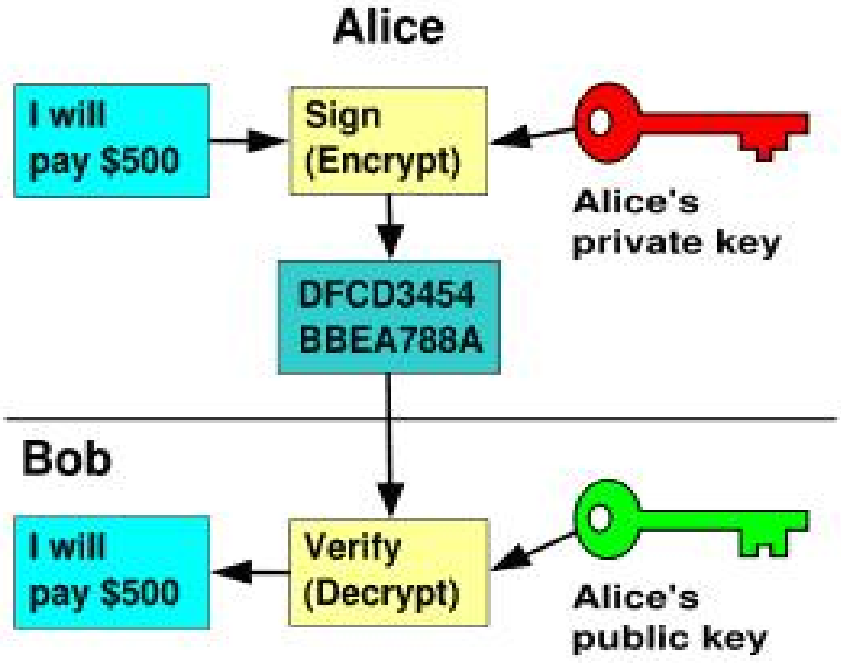
Výše rozebrané typy prostého elektronického podpisu představují pouze výčet nejčastěji používaných a dosud právní praxí rozeznaných. Je však bez pochyby možné, že v souvislosti se stále se rozvíjejícím technologickým pokrokem a zvyšující se četnosti užívání elektronických podpisů se v nejbližších letech tento výčet rozšíří o několik dalších forem, které budou postaveny na roveň podpisům vlastnoručním. Každá takováto nová forma podpisu však musí splňovat určité funkce vzhledem k písemnému vyjádření. Soubor těchto funkcí vymezuje kupříkladu německá právní nauka, a to v Návrhu zákona, jímž se mění formální požadavky soukromého práva

[11] Dostupné z: https://upload.wikimedia.org/wikipedia/commons/b/bd/Hancisjui.jpg, cit. [25. 4. 2018].

a další předpisy o moderních právních transakcích ze dne 14. 12. 2000[12] a jedná se o následující:

- uzavírací= podpisem listiny je stvrzena konečnost projevu vůle podepisujícího a naplněn jeho záměr
- zvěčňovací= projev vůle podepisujícího je trvale zachycen, dochází k vyloučení krátkodobé účinnosti takového úkonu
- identifikační= podpis zajišťuje jednoznačné a nezaměnitelné spojení s osobou signatáře
- autentičnosti= vyjádření spojitosti mezi dokumentem a podepisující osobou
- ověřovací= tato funkce je úzce spojená s funkcí identifikační a funkcí autentičnosti, umožňuje ověření pravosti podpisu skrze porovnání s tzv. podpisovým vzorem
- důkazní= podpis může sloužit jako důkazní prostředek
- varovací= poukázáním na zvýšenou právní závaznost dochází k uvědomění, varování podepisující osoby

[12] Drucksache 14/4987. Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr. Deutscher Bundestag, 14. 12. 2000. str. 16-17, dostupné z: http://dip21.bundestag.de/dip21/btd/14/049/1404987.pdf, cit. [11. 6. 2018].



Obrázek 1 – princip fungovánídigitálního podpisu

2.2. Dynamický biometrický podpis

Dynamickému biometrickému podpisu je v současnosti nejen odbornou veřejností věnována velké pozornost a je stále častěji používaným typem elektronického podpisu. Otázkou zůstává, zda se jedná o další zvláštní typ elektronické identifikace osob nebo jej lze zařadit pod kategorii elektronických podpisů prostých spolu s několika dalšími. Vzhledem k tomu, že dosavadní nauka uznává především druhý zmíněný způsob, rozhodla jsem se též tuto kategorizaci zachovat, z důvodu vysoké míry specifičnosti a stále rostoucího významu však považuji za vhodné přidělit tomuto podpisu vlastní, oddělenou kapitolu. Navíc je nutné připomenout i skutečnost, že dynamický biometrický podpis není pouhým otiskem rukopisu podepisujícího, obsahuje i záznam o rychlosti, jakou byl podpis vytvořen, způsob držení nástroje určeného k podepsání i velikost tlaku, který byl při podepisování vyvíjen na podložku. Z tohoto úhlu pohledu se tedy jedná o jakousi „vyšší formu“ prostého elektronického podpisu, je totiž nasnadě, že tak obsáhlý a komplexní soubor dat nelze srovnávat například s pouhým oskenovaným vlastnoručním podpisem nebo na klávesnici několika znaky zadanými na klávesnici. Nelze jej však podřadit pod kteroukoliv z nadřazených kategorií (uznávaný či kvalifikovaný elektronický podpis), jelikož jejich

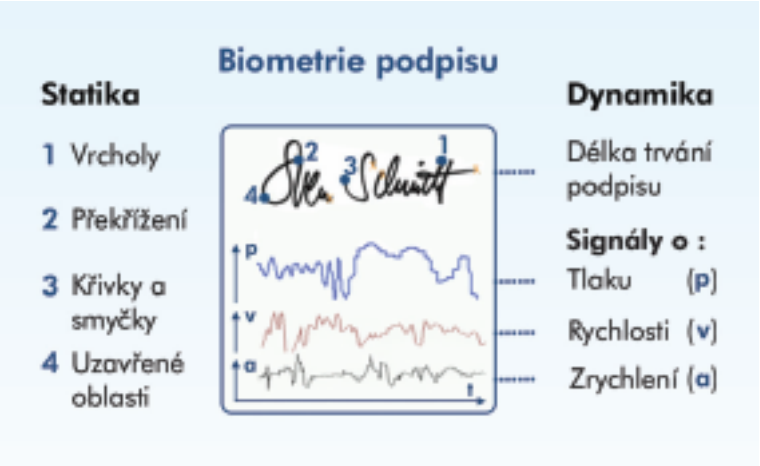
náležitosti nesplňuje. Dalo by se tedy shrnout, že se jedná o jakousi zvláštní, částečně mimo stojící kategorii elektronického podpisu.

Ač stále existuje mnoho skeptických názorů na bezpečnost a uznání tohoto typu podpisu, jeho platnost se dá odvodit výkladem za požití metody *per analogiam* z článku 3 odst. 10 nařízení eIDAS, v němž je vymezena definice elektronického podpisu. Dynamický biometrický podpis představuje též: „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání*“[13].

Jak jsem již naznačila, dynamickým biometrickým podpisem rozumíme nejen snímek podpisu podepisující osoby, ale i záznam o rychlosti, jakou byl podpis vytvořen, způsob držení nástroje určeného k podepsání, velikost tlaku, který byl při podepisování vyvíjen na podložku, celkovou velikost podpisu, délku a úhel čáry, počet smyček, oblouků a křivek, stejně jako případné zrychlení či zpomalení v jednotlivých bodech podpisu (pro ilustraci připojuji Obrázek 2[14]). Tento podpis se vytváří na speciální podložky – dotykové plochy, obvykle tabletu nebo jiných obdobných mobilních zařízení a v dnešní době je možné se s ním setkat například při podpisu převzetí zásilky od poskytovatele přepravních služeb, při podpisu smluv na pobočkách bank či různých operátorů. Veškerá data sebraná při vytvoření dynamického biometrického podpisu jsou následně zašifrována pomocí veřejného klíče, který by měl zabránit jejich zneužití a znemožnit přístup jiným než oprávněným osobám. Dešifrování je následně umožněno při zadání privátního klíče, který může být pro zvýšení míry právní jistoty uložen například u notáře a upotřeben v případě potenciálně nastalého soudního nebo jiného obdobného sporu o pravost dynamického biometrického podpisu.

[13] čl. 3 odst. 10 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

[14] SignoSoft [online]. [cit. 1. 5. 2018]. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php



Obrázek 2 – data získaná z dynamického biometrického podpisu

2.3. Elektronická pečeť

Elektronickými pečetěmi rozumíme podle článku 3 odst. 25 eIDAS: „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu*“[15]. V tomto ustanovení je účel těchto identifikátorů zcela jasně vymezen, jedná se tedy o nástroje, poskytující důkazy o tom, že určitý elektronický dokument vydala určitá právnická osoba a dále tento dokument nebyl žádným způsobem po jeho opatření elektronickou pečetí pozměněn či upraven. Jak jsem již zmínila v úvodu kapitoly, elektronické pečeti jsou jakýmsi „nástupcem“ elektronických značek podle ZEP a jak shrnuje komentář k ustanovení článku 35 eIDAS jsou elektronické pečetě: „*de facto elektronickou značkou právnické osoby*“[16].

Úprava elektronických pečetí je v zásadě obdobná, jako úprava elektronických podpisů. V § 8 ZSVDET je vymezeno použití kvalifikovaných elektronických pečetí ve veřejnoprávní oblasti. Následující § 9 stanovuje povinnost připojení uznávané elektronické pečetě, kterou rozumíme: „*zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť*“, při pečetění elektronických dokumentů, kterými se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem její působnosti. I poslední ustanovení ZSVDET dotýkající se úpravy elektronických pečetí

[15] Čl. 3 odst. 25 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
[16] DONÁT, Josef. Nařízení eIDAS: komentář. V Praze: C. H. Beck, 2017. Beckovy komentáře.

(§ 10 ZSVDET) prakticky kopíruje ustanovení o elektronickém podpisu, když stanoví, že: „*K pečetění elektronickou pečetí lze použít zaručenou elektronickou pečeť, uznávanou elektronickou pečeť, případně jiný typ elektronické pečeti, pečetí-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 8 nebo § 9 odst. 1.*“, v tomto případě by se tedy pravděpodobně dalo použít i shodné označení tedy „elektronická pečeť prostá“.

Dalším ustanovením eIDAS, které se k elektronickým pečetím vztahuje, je potom článek 35, svým obsahem, opět v podobném stylu jako článek 25 eIDAS pro elektronické podpisy, upravuje povinnost uznávat právní účinky elektronické pečeti a zákaz jejího odmítání jako důkazu v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečetě. Komentář k výše uvedenému článku nařízení eIDAS dále předpovídá, že další využití elektronických pečetí bude s ohledem na elektronizaci veřejné správy zásadní. Jako příklad uvádí komentář k nařízení eIDAS možnost předložit při vyžadování výpisu z rejstříku trestů fyzické osoby místo listiny elektronický výpis s pečetí příslušné vydávající organizace[17]. Pečeť i v tomto případě potvrzuje původ elektronického výpisu a jeho integritu. Kromě tohoto stvrzení bude však třeba ještě identifikovat i konkrétní fyzickou osobu, a to připojením jejího elektronického podpisu. V této situaci však nastává zásadní problém v rozhodnutí pořadí připojení jednotlivých identifikátorů. Pokud bude nejprve dokument opatřen pečetí a následně podepsán, jedná se o úkon, kdy fyzická osoba příslušný dokument kontroluje a potvrzuje, že se seznámila se jeho obsahem (tedy i pečetí). V opačném případě však obdobný závěr vyvodit nelze, vzhledem k tomu, že pečeť lze připojit i automatizovaně.

I v oblasti elektronických pečetí je nutné zmínit již dříve prezentovanou dvouletou přechodnou lhůtu. V tomto případě má období zajistit plynulý přechod a nahrazení uznávaných elektronických značek elektronickými pečetěmi. Po stanovenou dobu dvou let budou moci elektronické značky podle ZEP zastoupit elektronické pečetě a být tedy použity na jejich místě.

[17] DONÁT, Josef. Nařízení eIDAS: komentář. Praha: C. H. Beck, 2017. Beckovy komentáře.

3. Technologie elektronických identifikátorů

V následující kapitole se pokusím podrobněji přiblížit technologickou stránku elektronických identifikátorů. Ráda bych tento fenomén přiblížila všem, kteří jsou v technické oblasti spíše laiky, srozumitelným a názorným způsobem i ze stránky opačné, než je pouze ta právní. Vzhledem k tomu, že sama nejsem v tomto odvětví nijak zvlášť zkušená, budu se snažit o to, abych získané informace přetransformovala do této práce v co nejsnáze pochopitelnější formě, a to nejen formou podrobných popisů, ale i četných nákresů či vložených obrázků.

Pro sběr dat, jež jsem využila při tvorbě této kapitoly jsem využila zejména konzultací s odborníky v oblasti informačních technologií. Osobní vysvětlení bylo při snaze o pochopení nejen povahy elektronických identifikátorů jako takových, ale i mechanismů různých způsobů šifrování, velkou měrou účinnější než pouhé samostudium a snaha o proniknutí do problematiky skrze psaný text.

3.1. Elektronický podpis

Následující část práce se bude zabírat rozborem identifikátorů, které by v souladu s v předchozí kapitole uvedeným vymezením měly být označovány jako podpisy digitální, tvořící pouze poddruh skupiny takzvaných podpisů elektronických. Pro lepší uchopitelnost a snazší pochopení jsem však zvolila sice věcně nesprávný, ale obecně přijímaný termín elektronický podpis, a to i vzhledem k tomu, že právě toto terminologické rozlišení není základní podstatou následujícího textu.

Samotný elektronický podpis je ve své podstatě číselným kódem. Jako všechny elektronicky čitelné instrumenty je i tento kód tvořen tzv. binárním číslem, tedy kombinací binárních hodnot, které se v praxi nejčastěji zapisují jako 1 a 0. Tyto znaky mohou znázorňovat nejen základní pojmy pravda – nepravda (v pořadí 1-0), ale především i dva základní stavy elektrických obvodů a to zapnuto – vypnuto (opět ve shodném pořadí). V některých případech se pro odlišení od soustavy dekadické, tedy desítkové, používá místo klasické číslovky 1 znaku |.

Tato posloupnost znaků 1 a 0 tvoří ve výsledku kód, jehož zápis je tzv. zápisem pozičním, tedy záležícím pouze na pozici daného symbolu, což je zřejmé i z toho, že máme k dispozici pouze dva možné znaky. Obdobně se zapisují kódy například za použití Morseovy abecedy. Do binární soustavy je tedy možné, stejně jako právě do

Morseovy abecedy, převést jakýkoliv text. Například spojení Univerzita Karlova bude po přepisu do binárního kódu vypadat následovně:

01010101011011100110100101110110011001010111001001111010011010010111010001100001001000000100101101100001011100100110110001101111011011001100001.

Zápis elektronického podpisu pouze pomocí binárního kódu by však byl velmi nepraktický a vyžadoval by mnohonásobně větší počet použitých řádků. Zejména proto se v praxi provádí převod na textový řetězec. Tento řetězec může mít po převodu například takovouto podobu:

IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4Blrcnjaqbc KgNv+a5kr4537y8RCd+RHm75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAelws4S87UX80cLBtBcN6AACf11qymC2h+Rb2 j5SU+rmXWru+=QFMx.[18]

Výše uvedený řetězec je již sám o sobě příkladem zakódovaného elektronického podpisu, který byl vytvořen následujícím postupem. V první řadě je zpracován sám dokument, jenž má být opatřen elektronickým podpisem. Z tohoto dokumentu je vytvořen otisk, tzv. hash, který má fixní velikost. Tato velikost závisí na užité hashovací funkci a může být tedy např. 160 nebo až 512 bitů. Výhodou takového převodu dokumentu není tedy jen tvorba bloku dat o pevné velikosti, ale i jeho mnohonásobné zmenšení. Vytvořit otisk je totiž možné i u dokumentů, jejichž velikost je několik megabytů a se zpracovaným otiskem (hashem) se následně mnohem lépe pracuje v dalších procesech. Nejpoužívanějšími hashovacími funkcemi je v současnosti třída SHA-2 (zkratka SHA je tvořena počátečními písmeny slov Secure Hash Algorithm, tedy v překladu z angličtiny bezpečný hashovací algoritmus a číslovka 2 vyjadřuje pořadí), jíž tvoří funkce nazvané SHA-256, SHA-512, SHA-384 a SHA-224. Tato rodina hashovacích funkcí nahradila svou předchůdkyni SHA-1. Tato funkce byla definitivně prolomena na počátku loňského roku (tedy roku 2017), avšak její bezpečnost byla zpochybněna již v roce 2005, kdy se počaly objevovat první úspěšné útoky, v návaznosti na něž se například společnost Google rozhodla k ukončení jeho podpory ve třech postupných krocích a následnému přechodu na novou, stabilnější

[18] PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-3-8, str. 29.

funkci SHA-2. Pro doplnění uvádím, že funkčnost hashovací funkce spočívá v tom, že při jejím použití může docházet k tzv. kolizi. Takovou kolizí rozumíme situaci, v níž dochází k vytvoření stejného hashe ze dvou naprosto odlišných zpráv. Kromě výše zmíněných rodin SHA se v praxi užívají též metody Tiger nebo Message-Digest Algorithm.

V důsledku tohoto postupu je tedy vlastně podepisován ne samotný dokument, ale pouze jeho otisk – hash.

Vytvořený otisk se v dalším kroku zašifruje pomocí tzv. privátního klíče, ten ve své podstatě umožňuje samotný vznik elektronického podpisu a na druhé straně tzv. veřejný klíč následně zajišťuje jeho dešifrování. Po aplikaci prvního ze zmíněných klíčů získáme z otisku podepisovaného dokumentu právě textový řetězec, jehož příklad je uveden výše. Privátní klíč je soukromým, a tedy chráněným prostředkem, který by podepisující neměl poskytovat žádným dalším osobám, a to z důvodu zachování zaručení integrity a pravosti podepisovaných dokumentů. Jeho aplikací je dokončen proces vzniku elektronického podpisu.

Dalším krokem následujícím po zašifrování a připojení podpisu je zákonitě rozšifrování. Toho docílíme aplikací veřejného klíče. Veřejný klíč tvoří data, která jsou buď veřejně přístupná a nebo případně adresátovi zaslána osobou, která provedla zašifrování dokumentu pomocí privátního klíče. Jak jsem již uvedla výše, celý tento proces aplikace dvou různých typů klíčů je označován jako asymetrická kryptografie. Asymetrie této metody vychází ze skutečnosti, že je založená na tzv. jednocestných funkcích, jejichž provedení jedním směrem je výrazně jednodušší než opačný postup. Jsou tedy velmi obtížně, ač ne nemožně, invertovatelné. Dá se tedy velmi zjednodušeně říci, že veřejný klíč je jakýmsi „návodem“ jak poskytnutá data zašifrovaná pomocí soukromého klíče přečíst.

Aplikace tohoto typu šifrování umožňuje zjistit integritu elektronicky podepsaného dokumentu. Pro ověření pravosti a nezměněnosti zasílaného dokumentu postačí, pokud bude zaslaný otisk zašifrovaný soukromým klíčem prostřednictvím aplikace veřejného klíče dešifrován a porovnán s nově vytvořeným otiskem příchozí zprávy. V případě, že se oba (původní zašifrovaný a následně rozšifrovaný pomocí soukromého a veřejného klíče a nově na základě příchozí zprávy vytvořený) otisky absolutně shodují, je možné učinit závěr, že zprávu skutečně poslala daná osoba a v průběhu jejího doručování s ním nebylo žádným způsobem manipulováno.

3.2. Uznávaný elektronický podpis

Vyšší formou elektronického podpisu oproti v předchozí části popsanému podpisu digitálnímu (označovaného pro snazší uchopitelnost jako podpis elektronický) je elektronický podpis uznávaný, který je soukromoprávní podepisující povinen použít při jednání s orgánem veřejné moci. Tento druh podpisu je založen na podobném principu jako podpis digitální, avšak jeho důvěryhodnost a průkaznost osoby signatáře, stejně jako nezměnitelnost dokumentu jím opatřeného je založena kvalifikovaným certifikátem, který vydá certifikační autorita, tedy kvalifikovaný poskytovatel služeb vytvářejících důvěru.

Certifikátem pro elektronický podpis je podle čl. 3 odst. 14 nařízení eIDAS „*elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby*“. Jedná se tedy ve své podstatě o informaci, že konkrétní veřejný klíč patří konkrétní osobě, která je zároveň i držitelem příslušného klíče privátního. Veřejný klíč přímo do certifikátu vložen. Co se týče přímo kvalifikovaných certifikátů, jedná se potom podle čl. 3 odst. 15 eIDAS o takové certifikáty, které „*který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I*“. Pro úplnost doplním, že kromě kvalifikovaných certifikátů existují ještě certifikáty komerční, jejichž podobu ani užívání legislativa podrobněji neupravuje.

Kvalifikovaným poskytovatelem služeb vytvářejících důvěru je v souladu s ustanovením čl. 3 odst. 20 nařízení eIDAS „*poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele*“. Tito poskytovatelé jsou dle informací zveřejněných na internetových stránkách MV České republiky tři, a to sice První certifikační autorita, a.s., Česká pošta s.p., jejíž služba nazvaná Post Signum je v této oblasti pravděpodobně nejvyužívanější a dále potom společnost eIdentity, a.s.

Samotné kvalifikované certifikáty se uchovávají ve formátu X.509, který představuje standard pro systémy založené na veřejném klíči. Data v certifikátech nich obsažená jsou popsána jazykem ASN 1 (Abstract Syntax Notation One) a jedná se zejména o identifikační údaje majitele certifikátu, algoritmus použití pro vytvoření elektronického podpisu, identifikační údaje vydavatele certifikátu, počátek a konec jeho platnosti a vlastní otisk certifikátu prokazující jeho neporušenost.

Jejich šifrování funguje na složitosti hledání společného dělitele dvou velmi dlouhých prvočísel. Jedním z těchto prvočísel je právě tzv. veřejný klíč a druhým ten soukromý. prvočísla jsou vzájemně vynásobena a jsou touto operací natolik změněna, že jediným způsobem, jak je vrátit zpět do původní podoby, je provedení shodné operace opačným směrem, k čemuž je potřeba právě minimálně jedno z čísel, a to sice veřejný klíč. Pokud se podaří operaci provést a data mohou být přečtena, je zřejmé, že dokument skutečně podepsala osoba, která je vlastníkem klíče soukromého. Pokud by se někdo pokusil zfalšovat elektronický podpis například použitím veřejného klíče, operaci by se nepodařilo provést, data nemohla být přečtena a bylo by zřejmé, že se jedná o pouhý pokus kopie podpisu. Stejný výsledek by mělo i zfalšování podpisu použitím jakéhokoli jiného náhodného čísla.

Další podrobnější rozbor fungování kvalifikovaných certifikátů pro elektronické podpisy je nad rámec této práce. Jsem přesvědčena o tom, že výše uvedené informace spolu se shrnutím, že kvalifikovaný certifikát zaručuje totožnost podepisující osoby a jedná se o data připojená k jeho veřejnému klíči, která v situacích, kdy nedošlo k předání veřejného klíče mezi podepisující osobou a adresátem, ale například byl tento klíč připojen k podepisovanému dokumentu nebo zveřejněn on-line, stvrzují, že veřejný klíč skutečně patří dané osobě (tuto informaci zajišťuje třetí, nezávislá osoba, označovaná jako certifikační autorita), plně dostačují pro účely diplomové práce na právnické fakultě.

3.3. Dynamický biometrický podpis

Posledním elektronickým identifikátorem, kterým bych se ve své práci ráda zabývala, je dynamický biometrický podpis. Jeho stručnou charakteristiku jsem provedla již výše, pro připomenutí pouze uvádím, že se jedná o podpis vytvořený na elektronické čtecí zařízení vlastnoručně a zahrnuje tedy kromě grafické podoby podpisu i biometrické údaje o osobě podepisujícího.

Hlavní odlišností tohoto typu podpisu od výše podepsaných je jeho relativně snazší oddělitelnost od podepisovaného dokumentu. Dynamický biometrický podpis může, na rozdíl od toho elektronického existovat nezávisle na jiných datech. V důsledku je tedy možné čistě teoreticky umístit dynamický biometrický podpis na zcela prázdný list, snímání vlastnoručního podpisu z podložky není na žádných již existujících datech závislé.

Dynamický biometrický podpis je nutné odlišit od podpisů statických, tedy takových, které byly provedeny nikoliv na elektronickou čtecí podložku, ale pouze na obyčejný papír a následně pomocí skeneru převedeny do elektronické podoby. Z takových podpisů je také možné získat určitá data o jimi se podepisujících osobách, avšak jejich počet a kvalita je výrazně nižší oproti podpisům dynamickým. Statické podpisy jsou v některé literatuře též označovány jako tzv. off-line podpisy.

Co se týče technologie jejich vzniku, opět se zde setkáváme s asymetrickou kryptografií. Biometrická data jsou získána při podpisu na elektronickou čtečku a následně v zařízení zašifrována pomocí veřejného klíče. Tato zašifrovaná data jsou uložena do dokumentu ve formátu PDF a následně pomocí výše zmíněného algoritmu SHA-256 program vytvoří hash. Postup je tedy velmi podobný jako u tvorby elektronických podpisů.

Veškerá získaná biometrická data jsou bez prodlení zašifrována a jejich nezašifrovaná podoba se v žádném případě do paměti neukládá, aby se zamezilo případnému zneužití a zisku tzv. podpisového vzoru neoprávněnou osobou.

Údaje, které jsou při tomto způsobu podepisování získávány, jsou nejčastěji čtyři, a to sice grafická podoba podpisu, tedy vlastně „obrázek“, který je získáván i při podepisování statickém a veškeré jeho podrobnosti (vrcholy, smyčky, překřížení), rychlost podepisování, zrychlení a tlak, který je vyvíjen na podložku podpis snímající. V případech, že je podepisováno speciálním elektronickým perem, je možné získat i další údaj o signatáři, a to stisk, který je vyvíjen přímo na tuto pomůcku. Všechny tyto aspekty mohou být následně podrobněji rozpracovány a poskytnout tak další informace. Je možné zaznamenávat například i minimální a maximální rychlost, jíž podepisující podpis vytváří nebo náklon a natočení speciálního elektronického pera užitého k podepisování. [19]

3.3.1. Zařízení

Snímání biometrie dynamického podpisu je funkcí, kterou podporují pouze některé druhy elektronických zařízení. Nutnost jejich pořízení a velmi častá nedůvěra běžných uživatelů k tomuto typu podepisování jsou pravděpodobně hlavní

[19] SMEJKAL, Vladimír, KODL, Jindřich a Miroslav UŘIČAŘ. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*. [Online]. 2015, č. 11, s. 189. [cit. 20. 6. 2018]. Dostupné z: https://journals.muni.cz/revue/article/view/3586.

brzdou rozvoje tohoto typu podepisování, což je v každém případě škoda, vzhledem k tomu, kolik nesporných výhod přináší. Jednou z nich je například absolutní absence speciálních postupů na straně podepisujícího, který pouze aplikuje stejný postup jako při podepisování běžnými psacími potřebami na papír nebo rychlé ověření podpisu bez vysokých nároků na velikost místa uložení příslušných dat.

Co se týče samotných k zaznamenání dynamického biometrického podpisu potřebných zařízení, nejčastěji používanými a nejlépe pro tyto účely fungujícími jsou tzv. podpisové podložky neboli signpady. Jedná se o zařízení vybavené odolnou psací plochou, které díky úplné absenci hran a vyvýšených okrajů umožňuje pohodlné podepisování srovnatelné s psaním na běžný papír. Některé vyspělejší signpady umožňují i zobrazení podepisovaného dokumentu ve formátu PDF, u těch základních displej úplně chybí a poskytují pouze prostor pro zaznamenání podpisu. Hlavní výhodou těchto podpisových podložek je integrované šifrování. Podpis na ně vytvoření je okamžitě zašifrován, nejčastěji pomocí šifer RSA nebo AES.

Příslušenství signpadů tvoří tzv. stylus neboli elektronické pero, který může fungovat a s podložkou komunikovat například na principu elektromagnetické rezonance. Součástí pera je potom obvod, jehož nedílnou součástí je navinutá cívka. Tento obvod je naladěný na stejnou frekvenci, jíž produkuje generátor harmonického napětí umístěný pod povrchem psací plochy podpisové podložky. Výše zmíněná elektromagnetická rezonance vzniká při vyrovnání kmitočtů obou obvodů. Díky tomuto principu reaguje podložka na stylus nejen při samotném doteku, ale i při přiblížení těsně k povrchu.

Další zásadní výhodou těchto zařízení je kromě výše zmíněné šifrovací funkce například i skutečnost, že díky principu elektromagnetické rezonance jsou vyloučeny nechtěné doteky podložky například hranou ruky, které by mohly způsobit chybné zaznamenání dotyku mimo linku vlastního podpisu a při běžném podepisování potom například rozmazání textu.

Nejběžněji na českém trhu dostupnými jsou podpisové podložky vyrobené německou společností Signotec. Ta se kromě vlastní výroby signpadů zabývá i tvorbou softwarových aplikací, které umožňují podepisování na dalších zařízeních. Dalším velmi známým výrobcem, který nabízí svá zařízení na našem území je Wacom, japonská společnost založená roku 1983, jejímž nejznámějším produktem jsou grafické tablety. Signpady jsou dnes již běžně užívaným nástrojem, se kterým se můžeme

v běžném životě setkat takřka denně, používají je ve velkém i banky a pojišťovny, mimo jiné například MONETA Money Bank nebo pojišťovna Kooperativa.

Dynamické biometrické podpisy nemusí být vytvářeny jen na signpadech. Jak jsem již naznačila, například společnost Signotec se zabývá kromě jejich výroby i vývojem softwarových aplikací, které umožňují tvorbu podpisů i na dalších přístrojích. Po jejich instalaci je tedy možné využít možnosti tvorby podpisu například na některém z následujících zařízení. Pokud by na těchto zařízeních nebyl příslušný software nahrán, bylo by sice možné vytvořit „obrázek“ vlastnoručního podpisu, avšak nemohlo by dojít k zaznamenání jakýchkoli biometrických údajů a žádné údaje by nebylo možné při takovémto podepisování zašifrovat, vzhledem k tomu, že tyto přístroje samy o sobě takového postupu nejsou schopny.

Dynamický biometrický podpis je možné zaznamenat právě zmiňované grafické tablety. Jedná se o zařízení, která ke své práci využívají především grafici či fotografové při úpravě svých snímků. Jsou uzpůsobená ke kreslířským pracím a detailním retuším, které by dotek zprostředkovaný přes myš nebo touchpad notebooku nebyl schopen přesně provést. Grafické tablety mohou být vybaveny displejem, případně je možné je připojit k obrazovce počítače, na níž se výsledek pohybu na dotykové ploše přináší. Nutným příslušenstvím tohoto zařízení je též stylus fungující na stejném principu jako u výše popsaných podpisových podložek. Tablet je tedy schopen též zaznamenat nejen grafickou podobu podpisu, ale i další atributy jako vyvíjený tlak nebo náklon elektronického pera při jeho provádění. Nejrozšířenějšími grafickými tablety na tuzemském trhu jsou již výše zmíněná zařízení japonské značky Wacom.

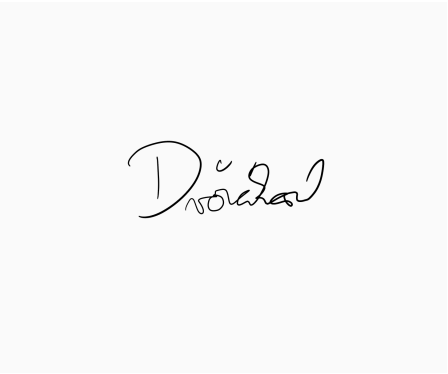
Zvláštním přístrojem, který by se dal označit za jakéhosi hybrida schopného zastoupit funkčnost jak grafických tabletů nebo signpadů, tak i klasických tabletů nebo notebooků je Yoga Book od společnosti Lenovo, největšího světového výrobce počítačů. Toto zařízení bylo představeno v září roku 2016 a jedná se o zcela přelomový nástroj. Yoga Book vypadá na první pohled jako velmi tenký notebook, který se oproti těm klasickým liší zejména tím, že není vybaven mechanickou klávesnicí, ale pouze virtuální, která se však umí zároveň změnit i na dotykovou plochu, na níž je možné psát elektronickým perem. Stylus je součástí příslušenství každého Yoga Booku a právě jeho prostřednictvím je možné vytvořit dynamický biometrický podpis. Princip fungování je stejný jako u grafického tabletu, napsaný text se nezobrazuje přímo na podpisové ploše, ale na displeji zařízení. Podobně jako u výše uvedených zařízení je Yoga Book schopen zaznamenat na stylus i podložku vyvíjený tlak,

a to podle údajů výrobce až v 2048 různých úrovních přítlaku. Obrovskou výhodou Yoga Booku je možnost připnout k dotykové ploše blok, vyměnit pasivní hrot elektronického pera za ten inkoustový a psát klasicky na papír, avšak s tou výhodou, že i tak se vytvořené linie přenesou skrze dotykovou oblast na displej tabletu. Jedná se tedy vlastně o jakousi kombinaci klasického psaní na papír a moderního záznamu skrze speciální elektronické pomůcky.

Yoga Book je v současnosti pro svou multifunkčnost a pravděpodobně i velmi elegantní vzhled a nízkou celkovou váhu hojně využívaným nástrojem. Ve velkém měřítku jej používá například společnost M&M Reality, která učinila zásadní krok, když své makléře oprostila od tradičních papírových smluv a spousty dalších dokumentů a vybavila je právě zařízeními Yoga Book. Na nich je možné nejen prezentovat veškeré podrobnosti o předmětné nemovité věci, ale zároveň přímo podepsat potenciálně uzavřenou smlouvu. Jedná se tedy o další zásadní krok v modernizaci a rozšiřování povědomí o elektronických podpisech, stejně jako zvyšování jejich důvěryhodnosti.

Kromě výše uvedených přístrojů je možné po instalaci příslušného softwaru vytvořit dynamické biometrické podpisy i na některých typech iPadů nebo telefonu Samsung Galaxy Note, které jsou vybaveny elektronickými pery.

Pro ilustraci grafické podoby podpisu zaznamenaného na Lenovo Yoga Book přikládám můj vlastní podpis na tomto zařízení pořízený. Vzhledem k tomu, že tento přístroj není vybaven vhodnou aplikací, která by byla schopna zaznamenat a zpracovat příslušné biometrické údaje, jedná se skutečně jen o pouhý „obrázek“ mého podpisu.



Obrázek 3 – vlastoruční podpis

4. Elektronická identifikace v praxi

Závěrečná kapitola mé práce se bude věnovat praktickému využití elektronických podpisů. Přiblížím v něm všechny okolnosti nutné pro vlastní použití této moderní technologie a pokusím se vytvořit praktický návod pro běžného uživatele.

Podle mého názoru rozšíření užívání elektronických identifikátorů brání z větší části právě určité obavy a nejistota, jež mohou být s tímto způsobem podepisování stále ještě spojeny. Ač naše společnost prochází velmi rychlou modernizací a například mobilní telefon či stolní počítač nejsou v žádném případě technologickými vymoženostmi, které by byly doménou pouze „mladých“, tedy osob přibližně do třiceti let věku, ale i lidem ve věku důchodovém už dnes běžně pošleme SMS zprávu nebo e-mail, existují stále určité fenomény, jimž se takový pokrok učinit nepodařilo.

Elektronické podpisy jsou dnes hojně využívány především v poměrech veřejnoprávních, kupříkladu při komunikaci se soudy se zasílají elektronicky podepsané dokumenty skrze datové schránky velmi často, avšak stále se jedná především o podání učiněná advokáty nebo jinými podobně odborně zainteresovanými osobami. V běžných soukromoprávních poměrech panuje ohledně elektronických identifikací určitá nejistota, způsobená z větší části i poměrně novou a dosud velmi často obměňovanou legislativou. Navzdory tomu, že elektronicky podepsaný dokument znamená větší dávku právní jistoty a zbavuje uživatele pochybností o pravosti a integritě daného dokumentu, stále je možné zaznamenat jisté pochybnosti, když například banka či poštovní doručovatel předloží klientovi k podpisu tablet nebo jiné elektronické zařízení namísto tradičního papíru a pera. Jako by snad propojení se světem technologií a elektronizace automaticky znamenalo pokus o nějaký podvod nebo zákeřnost a neviditelný svět „jedniček a nul“ uměl snáze takovéto nekalé praktiky skrývat.

Z výše uvedených důvodů bych ráda detailně popsala postup, který je nutný pro zajištění možnosti používání elektronických podpisů pro běžného uživatele. Jedná se vlastně slovy našich vrcholných politických představitelů o takovou „kuchařku, jak elektronické identifikátory v praxi používat“.

4.1. Prostý elektronický podpis

Jak může být již zřejmé z předchozích kapitol tohoto souboru, na použití prostého elektronického podpisu není třeba žádného zvláštního či expertního postupu.

S tímto typem elektronické identifikace se setkává drtivá většina z nás takřka denně a často si možná ani neuvědomujeme, že se naše jednání dá označit za elektronický podpis, aniž bychom podstupovali a vytvářeli nějaké složité počítačové operace nebo podobně komplikovaná jednání.

Při skenování vlastnoručního podpisu, případně celé listiny právě vlastnoručním podpisem opatřené možná někoho z podepisujících napadne, že dochází k jakési elektronizaci již provedeného právního úkonu a elektronický podpis tak může vzniknout. Oproti tomu v případě, kdy například při nákupu na e-shopu nebo registraci na některé ze sociálních sítí uživatel kliknutím na příslušné políčko a tím zvolením možnosti „Souhlasím“ s výše uvedeným textem, by mnoho z nich ani nenapadlo, že takové jednání může splňovat náležitosti prostého elektronického podpisu.

Dá se tedy říci, že pro použití většiny forem prostého elektronického podpisu není třeba žádného speciálního postupu, výjimku však tvoří již dříve částečně vyčleněný a podrobněji rozebíraný podpis digitální a dynamický biometrický. Co se týče jejich praktického užití, ač jsou *de lege lata* tyto formy řazeny na roveň výše specifikovaným typům, jako například pouhému podpisu v zápatí elektronické zprávy, v běžném životě bychom takovou rovnost hledali jen stěží. Ve skutečnosti je dynamický biometrický podpis, stejně tak jako digitální, hodnocený jako mnohem vyšší forma podpisu a mnoho společností dokumenty jimi opatřené uzná za elektronicky podepsané, na rozdíl od listin, které jsou například jen stvrzeny oskenovaným podpisem. Z tohoto důvodu bych jim ráda věnovala opět více prostoru a zařadila je do vlastních podkapitol.

4.1.1. Digitální podpis

Digitální podpis je založen na asymetrické kryptografii, tedy použití kombinace soukromých a veřejných klíčů. Pro jeho použití je tedy třeba nejdříve získat tyto dva klíče. Předem následujícího popisu postupu nutného pro jejich zisk upozorňuji, že je tento v praxi pro svoji komplikovanost téměř nepoužívaný a většina uživatelů upřednostňuje pořízení kvalifikovaného certifikátu pro elektronický podpis, vzhledem k tomu, že tento je jednoduše vygenerován a přiřazen certifikační autoritou. Nejen, že je tedy tento postup jednodušší, ale i váha podpisu opatřeného kvalifikovaným

certifikátem (tedy uznávaného elektronického podpisu) je mnohonásobně vyšší než pouhého podpisu digitálního.

Soukromý klíč získáme následujícím způsobem. Uživatelé zkušení v programování si jej mohou sami vygenerovat pomocí následujícího příkazu: $ openssl genrsa -out key.pem -aes256 4096. Takto vygenerovaný klíč bude mít velikost 4096 bitů a zašifrování bude provedeno pomocí šifry AES. Pokud však osoba nesplňuje výše specifikované požadavky a tento příkaz pro ni neznamená více než náhodnou změť nesmyslně poskládaných písmen, může pro takový účel využít některý ze specializovaných programů nebo on-line služeb. Po vygenerování dostane uživatel soukromý klíč, který může mít například takovouto podobu:

[20]-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgHvUzd0vgUxjrN1QMIpBVcASuhbRJ7ZgjYaKQd7JKlRHelt5o8gB
toQCLtHPIyvJJy+RjqRZ95rX0sztih1yDEHrsPC1vwXzycrhH6ln6ZM/1edF3Kog
o+OgtZQ8+0S05COkle5IVbVhgW8BWA4nnuaKYBs4vqu2uAdYe0DpOD5tAgMB
AAEC
gYBGVRTkBwJSR968CLq5G+i/YiONqBf9LxPTEZ3eErXXDo4BfLI4fDiU+8Rp6F
Na
oDKAgxTYZj0LFoAlYtlqZgdtcDuLy22WnG6idSs0JB1R0EFJhRmyKQcP2o1oPEZz
9WIoVgXc73MGoJC1iQH8S4m+/pK6JEQdxB0Msv4z2BmWxQJBANQaj6xxg2CH
y+ba
BY1vhzubTGVs7Z2TD2fc9fMOmN3PwD4pO5PXY0U7RHTbbp3DMWF9gDWPyr
jy8Iat
Z4vZ7sMCQQCVdX2lk6x4/bXblIlG1cBol1QcnOKZ7onrqJZozLJARs8WFKVopGF
P
/YaUABO5DRdR0mBsX0oFvDmx5LC1vasPAkEAl0NCB0cE3Ii736zInO9W0CmW
uBaQ
9vlz2Sx5spdMaZPJlAsv0+WdhDgaQARlxNj5lH8+OfSMLI4E/ucXm2MWpQJAY1g
n
XmncWMf7m6sN3IG0VVFRXXuCu+Ls1jHHWH3HdiYa/IhYskehT3QrgjDS60wiV
gbK
hP6Jy2ojx3VFaGhcTQJAROl2t3J9vfQ0luzFHEdFXLndfd8qvIN7svduq04v5dVe
7NfZAdUuo9/IXTymbExQLOWfWCZHfnD5kkTVg8P1Ew==

[20] Tento privátní klíč byl vygenerován dne 14. 6. 2018 prostřednictvím webových stránek dostupných na následujícím odkazu: http://travistidwell.com/blog/2013/09/06/an-online-rsa-public-and-private-key-generator/

-----END RSA PRIVATE KEY-----[21]

Tímto úkonem je vlastně těžší polovina procesu splněna. Veřejný klíč se totiž generuje z již vytvořeného soukromého klíče, a to stejně jako v prvním případě za použití speciálního příkazu (openssl rsa -in key.pem -out public.pem) nebo zjednodušeně s využitím programu nebo webové služby. Ve chvíli, kdy uživatel disponuje ji i klíčem veřejným, který může vypadat například takto:

-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgHvUzd0vgUxjrN1QMIpB
VcASuhbR
J7ZgjYaKQd7JKlRHelt5o8gBtoQCLtHPIyvJJy+RjqRZ95rX0sztih1yDEHrsPC1
vwXzycrhH6ln6ZM/1edF3Kogo+OgtZQ8+0S05COkle5IVbVhgW8BWA4nnuaKYB
s4
vqu2uAdYe0DpOD5tAgMBAAE=
-----END PUBLIC KEY-----,

disponuje již vším potřebným k tomu, aby mohl vytvářet digitální podpisy.

Znovu však upozorňuji na skutečnost, že tento postup je v porovnání s jeho důkazní váhou a využitelností natolik zbytečně komplikovaný, že se mu drtivá většina podepisujících raději vyhne a upřednostní některou z dalších forem elektronické identifikace, ať už se jedná o uznávaný elektronický podpis opatřený kvalifikovaným certifikátem pro elektronické podpisy nebo například dynamický biometrický podpis. Za zvážení stojí také fakt, že digitální podpisy jsou typem elektronického podpisu prostého, stejně jako například pouhé zadání PIN kódu nebo podepsání v e-mailu (tedy vlastně napsání vlastního jména skrze klávesnici) a mají tedy stejnou váhu s těmito instrumenty. Zde se bezesporu nabízí návrh na vylepšení stávající legislativy, kdy by bylo vhodné konečně nějak konkrétně vymezit, jaké typy podpisů zahrnují přesně formy a jaká je jejich použitelnost a důkazní hodnota. V soukromoprávním poměru tak záleží především na dohodě jednotlivých účastníků, jaká pravidla pro použití elektronických identifikátorů si sami nastaví.

4.1.2. Dynamický biometrický podpis

Nejasnosti se v praxi vyskytují nejčastěji, jak jsem uvedla již dříve, v souvislosti s dynamickým biometrickým podpisem. Tento typ podpisu by ve své podstatě mohl být,

[21] Na tomto místě si dovolím upozornit na zjevné využití šifry RSA, o níž jsem čtenáře informovala v úvodní kapitole této práce.

díky množství dat, které o podepisujícím získává a jejich okamžitému šifrování, jedním z nejpoužívanějších a nejváženějších vůbec, současná právní úprava se tomuto typu však, stejně jako drtivě většině těch ostatních, prozatím vyhýbá. Přitom dynamický biometrický podpis, jak je zřejmé z jednoduché úvahy nad touto problematikou, by měl být minimálně stejně, ne-li o stupeň výše postavený, jako podpis vlastnoruční. Jedná se přece o stejnou formu (tedy tahem ruky vytvořený obrázek), avšak v případě prvního zmíněného typu jsou zaznamenána četná přídavková data o podepisujícím. Z vlastnoručního podpisu je možné některá z nich získat též, ale pro tento případ by bylo nutné využít nejen časově náročných, ale i zásadně finančně nákladných služeb znalce v oboru písmoznalectví.

Příčinou této mezery v právu může být kromě nepružně reagující právní vědy například i domněnka o nedostatečném prozkoumání oblasti elektronické identifikace a relativně krátká doba, po kterou jsou tyto nástroje využívány. Do budoucna však snad bude i problematika tohoto odvětví lépe ošetřena a dojde na stanovení jasných pravidel pro užívání a uznávání elektronických identifikátorů.

Praktické využití dynamického biometrického podpisu není však ničím komplikovaným. Jak jsem již uvedla v předchozí kapitole, je k němu potřeba jen vhodné elektronické zařízení, které je pro snímání biometrie podpisu přímo uzpůsobeno nebo i jiný přístroj, do nějž bude software umožňující takovéto použití dodatečně nainstalován. První možnost z těchto dvou je samozřejmě o něco málo snazší, avšak otázkou zůstává, jak často bude takový přístroj, který umí pouze snímat biometrii dynamických podpisů, využíván. Proto je podle mého názoru pro užití v obchodních společnost, jakými jsou například banky nebo spořitelny, výhodnější nakoupit speciální čtečky těchto podpisů, tzv. signpady a dále se nezabývat sháněním a plošnou instalací speciálních programů. Na druhé straně, pokud je osoba, která zařízení pořizuje, pouze jedinec, bylo by pro ní takové zařízení pravděpodobně zbytečné a raději si pořídí některý z dále uvedených přístrojů, které může využívat i k dalším účelům, jako například v případě grafického tabletu digitální kresbě či ostatním funkcím, které zvládne Yoga Book, který se dá vlastně považovat za mini notebook, a následně si pořídí software, jehož instalace pro toto jedno zařízení nebude nijak nesnesitelně časově náročná.

Podepisující osoba též nemusí prokazovat žádné speciální vlastnosti a schopnosti, snad jen kromě potlačení strachu z elektroniky a překonání nedůvěry k elektronickým identifikátorům a samozřejmě schopnosti se samostatně

podepsat běžným způsobem, tedy inkoustem na papír. Jinak je provedení biometrického podpisu ve své podstatě jednodušší, například proto, že dotykové plochy reagují jen na stylus a není tak možné například dlaní rozmazat inkoust napsaného podpisu.

Co se týče nutnosti pořízení speciálního zařízení ze strany osoby, která podpis vyžaduje (tato situace je pravděpodobnější a v praxi rozhodně častější, nákup těchto zařízení uskutečňují především větší společnosti pro zvýšení efektivity práce svých zaměstnanců a zvýšení komfortu klientů) nebo přímo podepisujícího, nejedná se o nijak závratnou finanční investici. Signpady se dají pořídit za cenu okolo 3.000,- Kč, grafické tablety dokonce i o tisícikorunu levněji a ač vyžadují další investici v podobě nákupu speciálního software pro umožnění snímání dynamických biometrických podpisů, jedná se na druhé straně o zařízení, jehož využití je rozhodně širší než pouze pro tyto účely. Jedná se o pomůcku, jíž je možné použít například při úpravě fotografií nebo digitální malbě. Její pořízení je tedy výhodné především pro jedince, kteří mají v plánu působit v umělecké oblasti. Další z v předchozí kapitole zmíněných přístrojů byl Lenovo Yoga Book, jehož pořízení je již podstatně nákladnější, avšak jeho využití je ze zmíněných zařízení s přehledem nejširší. Tuto kombinaci notebooku, tabletu a grafického tabletu je možné zakoupit za cenu zhruba od 15.000,- Kč.

4.1.3. Uznávaný elektronický podpis

Ač je uznávaný elektronický podpis jedním z nejkomplikovanějších elektronických identifikátorů vůbec, jeho používání běžným uživatelem je poměrně snadné. Podepisující si musí pro podepisování tímto typem elektronického identifikátoru zajistit vystavení kvalifikovaného certifikátu pro elektronické podpisy. Tento postup ilustruji na příkladu služby Post Signum poskytované Českou poštou, s.p.[22]

Získat kvalifikovaný certifikát pro elektronický podpis je možné na pobočkách České pošty. Co se týče elektronických žádosti, ty jsou umožněny pouze žadatelům o tzv. komerční certifikáty. Tito žadatelé již navíc musí být vlastníky platného kvalifikovaného certifikátu. Tento postup je odlišný pro fyzické a právnické osoby, na rozdíl od ceny za přidělení kvalifikovaného certifikátu pro elektronický

[22] Dostupné na: http://www.postsignum.cz/postup_pro_ziskani_certifikatu.html

podpis, která je pro každý ze subjektů stejná a činí celkem 396,- Kč. Platnost takového certifikátu je omezena na 1 rok. V první řadě popíšu postup, který je vyžadován od prvních zmíněných, tedy osob fyzických.

Fyzická osoba uzavře s Českou poštou smlouvu o poskytování certifikačních služeb, jejíž znění je možné stáhnout ve formátu PDF na následující internetové adrese: http://www.postsignum.cz/fyzicke_osoby.html, stejně jako formulář, do nějž je nutné vyplnit údaje pro vydání certifikátu. Tyto dvě listiny zájemce o udělení kvalifikovaného certifikátu vyplní, vytiskne a podepsané odevzdá na pobočce České pošty se službou Czech POINT, na níž se musí dostavit osobně, není možné zastoupení ani zplnomocněným zástupcem. Spolu s těmito dvěma listinami odevzdá fyzická osoba žádost o certifikát, kterou je možné vygenerovat stejně jako párové klíče prostřednictvím programu Post Signum Tool Plus. Svou identitu na příslušné pobočce prokáže žadatel dvěma různými průkazy totožnosti, přičemž primární a obligatorně vyžadovaný bude občanský průkaz nebo cestovní pas. Pracovník České pošty následně vydá certifikát a předloží žadateli k podpisu Protokol o vydání certifikátu. Tento protokol obsahuje mimo jiné i heslo pro zneplatnění certifikátu, které je vygenerováno automaticky, avšak je možné požádat i o použití hesla vlastního. Posledním krokem záležejícím v úkonech žadatele o přidělení kvalifikovaného certifikátu pro elektronický podpis je jeho instalace do aplikace, z níž byly vygenerovány klíče. Spolu s instalací certifikátu je nutné instalovat i certifikáty certifikačních autorit. Po dokončení instalace se ze žadatele stal právoplatný držitel kvalifikovaného certifikátu pro elektronický podpis, který může nyní podepisovat dokumenty uznávaným elektronickým podpisem.

Dalším subjektem, který si může o přidělení kvalifikovaného certifikátu pro elektronický podpis požádat, je osoba právnická. Ta uzavírá s Českou poštou, stejně jako první popisovaný subjekt, smlouvu o poskytování certifikačních služeb, s tím rozdílem, že je v ní povinna uvést seznam pověřených osob, které budou danou právnickou osobu zastupovat v jednání s Post Signum. Další požadovanou listinou je potom opět shodně jako v předchozím případě formulář obsahující údaje pro vydání certifikátu a k němu navíc ještě úvodní list seznamu žadatelů, v němž je uvedeno, o jaké certifikáty bude příslušná právnická osoba žádat. Spolu s vygenerovanou žádostí o certifikát je opět nutné výše uvedené předat na pobočce České pošty, která poskytuje službu Czech POINT. Za právnickou osobu může jednat její zástupce, který kromě výše uvedených dokumentů předloží i doklad o IČ, pokud není daná právnická

osoba zapsána v některém z veřejných rejstříků a stejně tak doklad o jmenování statutárního zástupce v případě, že tuto informaci není možné zjistit výpisem z obchodního rejstříku. Zástupce se navíc musí prokázat alespoň jedním osobním dokladem totožnosti. V případě, že se právnická osoba při žádání o vydání kvalifikovaného certifikátu chce nechat zastoupit pouze svým zaměstnancem, je tento postup možný pouze v případě že již byla uzavřena smlouva o poskytování certifikačních služeb, zpravidla uzavíraná na dobu neurčitou, a zaměstnanec organizace přijde na pobočku pouze požádat o vydání certifikátu. Opět se prokáže jedním dokladem totožnosti a předloží vygenerovanou žádost o kvalifikovaný certifikát. Posledním krokem je shodně jako v předchozím případě instalace vydaného kvalifikovaného certifikátu pro elektronický podpis.

Posledním subjektem, který může o vydání kvalifikovaného certifikátu pro elektronický podpis žádat, je podnikající fyzická osoba. Postup se v tomto případě nijak výrazně neliší od toho, jenž musí absolvovat osoby právnické, jediným výrazným rozdílem je skutečnost, že podnikatel se na pobočku musí dostavit opět osobně, jako tomu bylo v případě žádosti podané fyzickou osobou. Všechny dokumenty musí předložit shodně, jako osoba právnická, pro shrnutí uvedu, že se jedná o vyplněnou a podepsanou smlouvu o poskytování certifikačních služeb, vyplněný formulář s údaji pro vydání certifikátu spolu s úvodním listem, doklad o právní subjektivitě, pokud není podnikající fyzická osoba zapsána v živnostenském rejstříku a vygenerovanou žádost o certifikát. Podnikající fyzická osoba se na pobočce České pošty (tato pobočka musí samozřejmě opět poskytovat službu Post Signum) prokáže při podávání žádosti jedním dokladem totožnosti. Závěrečný krok je i do třetice shodný s předchozími variantami, a i podnikající fyzické osoby svůj kvalifikovaný certifikát pro elektronické podpisy zprovozní jeho instalací do aplikace, z níž byly vygenerovány párové klíče a žádost o certifikát.

Jak jsem již předestřela výše, platnost takto vydaných certifikátu je omezena na jeden rok, po jehož uplynutí je nutné v případě zájmu o další používání uznávaných elektronických podpisů nutné požádat o vydání následného certifikátu, jelikož nedochází k automatické obnově. Následný certifikát je opět zpoplatněn a jeho platnost je prodloužena o 20 dní, tedy na celkem 385 dní. Žadatel o následný certifikát si znovu vygeneruje žádost o certifikát spolu s párovými klíči v příslušné aplikaci a skrze e-mail si může požádat o vydání následného certifikátu. Tato žádost musí obsahovat sériové číslo certifikátu k obnově, informaci o certifikační autoritě,

která certifikát vydala a informaci o tom, zda se jedná o osobní či technologickou certifikační politiku, kontakt na žadatele a v případě, že žadatel nemá zájem o použití automaticky vygenerovaného hesla pro zneplatnění i jeho vlastní návrh. Kompletně vyplněnou e-mailovou zprávu žadatel následně zašle na adresu podatelna.postsignum@cpost.cz a následně se již řídí instrukcemi v e-mailech zaslaných v odpovědi.

Ač takto podrobně popsaný postup může vypadat velmi komplikovaně, ve výsledku se jedná o vyplnění několika listin, vygenerování párových klíčů a žádosti, které zvládne sama aplikace a následnou osobní návštěvu na pobočce České pošty spolu s úhradou bez čtyř korun čtyřsetkorunového poplatku. Česká pošta jako certifikační autorita po absolvování tohoto postupu následně garantuje identitu podepisujícího jeho zařazením do seznamu vydaných kvalifikovaných certifikátů. Uznávaný elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis je tedy v soukromoprávních poměrech nejvyšším možným typem podpisu, pokud do tohoto srovnání neřadíme elektronické pečetě, které se v rámci tohoto pojetí dají považovat za zvláštní samostatnou kategorii.

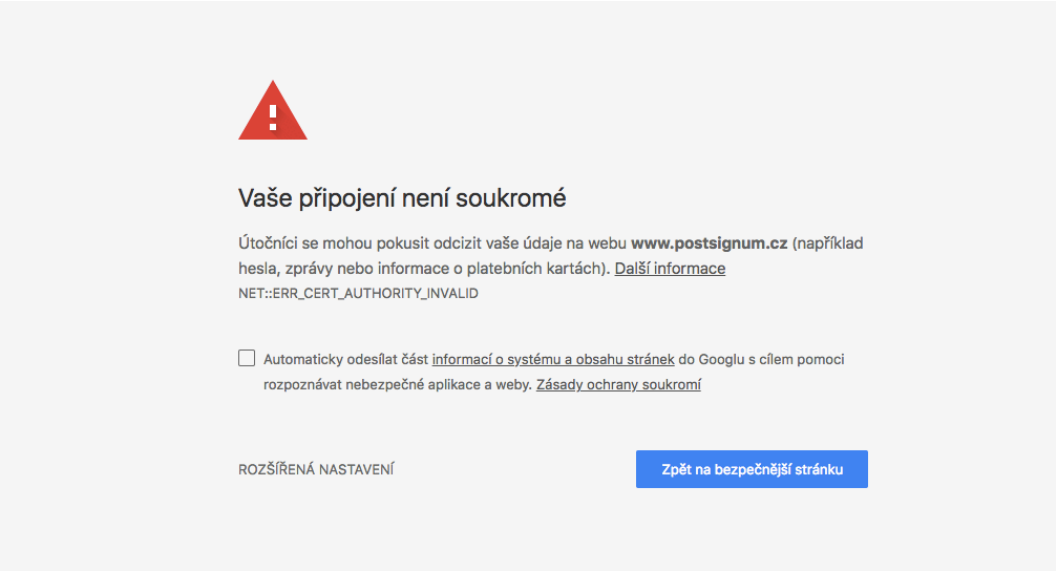
4.1.4. Elektronická pečeť

Elektronické pečetě jsou nástrojem, který umožňuje prokázat pravost a integritu daného dokumentu. Zásadním a nejvýraznějším rozdílem je omezení používání elektronických pečetí pouze na právnické osoby. Systém elektronických pečetí kopíruje, jak jsem rozebrala již v druhé kapitole této práce, systém elektronických podpisů. Podle čl. 8 ZSVDET odst. 1 má podepisující při jednání vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti povinnost použít uznávanou elektronickou pečeť. Ta je stejně jako uznávaný elektronický podpis založena na kvalifikovaném certifikátu pro elektronickou pečeť. V následující části této práce opět naznačím praktický postup nutný pro získání tohoto certifikátu a umožnění používání uznávané elektronické pečeti.

Udělení kvalifikovaného certifikátu provádí certifikační autority, stejně jako tomu bylo u certifikátů pro elektronické podpisy. Pro snadnější ilustraci popíšu znovu postup při žádosti o vydání certifikátu Českou poštou, tedy konkrétně její službou Post Signum. Každý žadatel musí být v první řadě držitelem kvalifikovaného certifikátu pro elektronický podpis Post Signum a musí se jednat o zástupce právnické osoby.

Znovu zdůrazňuji, že k užívání tohoto elektronického identifikátoru jsou oprávněny výhradně jen právnické osoby, tato služba není v současnosti fyzickým osobám, ať už podnikajícím či nepodnikajícím, zpřístupněna.

Podání žádosti může zájemce o udělení certifikátu uskutečnit buď prostřednictvím on-line systému nebo zasláním elektronicky podepsaného e-mailu. Před spuštěním on-line žádosti musí pověřená osoba organizace požádat v zákaznickém portálu Post Signum o přidání nových údajů pro vydání certifikátu pro elektronickou pečeť a tato žádost o přidání musí být autoritou potvrzena a schválena. Komplikací při této žádosti může být požadavek na používání operačního systému Windows a prohlížeče Internet Explorer. Pokud se žadateli podaří tyto podmínky splnit, vybere v průvodci nejprve svůj osobní certifikát Post Signum a dále vyplní požadované údaje pro vydání certifikátu pro elektronickou pečeť. Závěrečným krokem je potom již automatické vygenerování žádosti a zaslání do elektronické podatelny Post Signum. Vzhledem k tomu, že žadatel již zákonitě musí být držitelem kvalifikovaného certifikátu pro elektronické podpisy, není nutné ověřování jeho totožnosti fyzicky na pobočce České pošty. Celý průběh žádosti tak může být uskutečněn skrze internetový prohlížeč, kterým však musí být v dnešní době již běžnými uživateli minimálně využívaný Internet Explorer. Při pokusu o spuštění v prohlížeči Google Chrome na počítači s operačním systémem MacOS se objeví následující obrazovka:



Obrázek 4 – odepření přístupu neoprávněnému uživateli

Pokud žadatel zvolí druhou z nabízených možností a bude chtít o certifikát pro elektronickou pečeť požádat prostřednictvím elektronicky podepsaného e-mailu,

postup bude samozřejmě v části odlišný. Jeho počátek však zůstane shodný, pověřená osoba musí v zákaznickém portálu požádat o přidání nových údajů pro vydání certifikátu pro elektronickou pečeť a toto přidání musí být certifikační autoritou schváleno. Dalším krokem je vygenerování nových párových klíčů a žádosti o vydání certifikátu. Následně je nutné na elektronickou podatelnu Post Signum zaslat e-mail s požadovaným obsahem, jenž bude tvořit název právnické osoby, která o vydání certifikátu žádá, číslo uzavřené smlouvy o poskytování certifikačních služeb, jméno žadatele o certifikát, číslo zaměstnance v organizaci, kontaktní údaje žadatele a následně ID žádosti o certifikát, pokud nebude tato připojena k e-mailu jako příloha ve formátu REQ. Stejně jako v případě žádosti o certifikát pro elektronické podpisy je nutné uvést vlastní heslo pro zneplatnění certifikátu, pokud žadatel nechce využít automaticky vygenerované heslo, jež mu poskytne certifikační autorita. Celý takto sestavený e-mail je nutné elektronicky podepsat. Post Signum nespecifikuje požadavek na typ elektronického podpisu, jímž musí být zpráva opatřena, avšak z požadavku na předchozí dispozici s kvalifikovaným certifikátem pro elektronické podpisy lze předpokládat, že služba bude trvat na připojení uznávaného elektronického podpisu. Po odeslání e-mailu bude žadatel dále postupovat v souladu s pokyny zaslanými v odpovědi ze strany služby Post Signum.

Cena kvalifikovaného certifikátu pro elektronickou pečeť je podstatně vyšší než cena za certifikát pro elektronické podpisy. Za certifikát platný po dobu jednoho roku zaplatí podepisující částku ve výši 780,- Kč. Co se týče cen za certifikáty obecně, služba Post Signum nabízí možnost uplatnit při platbě množstevní slevu. Zákazník, který v kalendářním roce požádá a uhradí více než 50 různých kvalifikovaných certifikátů, splní podmínky pro cenové zvýhodnění. Takové zvýhodnění bude uplatněno jako procentuální sleva ze základní ceny kvalifikovaného certifikátu, která se bude zvyšovat v přímé úměrnosti s počtem celkově odebraných certifikátů. Pro konkrétní cenová zvýhodnění je nutné kontaktovat přímo pracovníky služby, a to na některém z kontaktních e-mailů zveřejněných na internetové adrese http://www.postsignum.cz/certifikaty.html. Pro prodloužení platnosti kvalifikovaného certifikátu pro elektronickou pečeť, tedy vystavení certifikátu následného, je nutné vykonat shodný postup, jaký jsem popsala výše při rozboru žádosti o vydání následného certifikátu pro elektronické podpisy.

Závěr

Na závěr své diplomové práce, jejímž tématem byla elektronická identifikace osob v soukromoprávních poměrech, bych ráda shrnula průběh jejího vzniku a zhodnotila dosažení v úvodu vymezených cílů a záměrů. Téma jsem zvolila z důvodu, že jsem se chtěla pokusit vytvořit dílo, které bude znamenat alespoň minimální přínos v probírané oblasti a nebude jen znovu pojednávat o problematice několikrát řešené. Elektronická identifikace je problematikou, která v současnosti vyvolává spíše otázky a zároveň obavy z jejího skutečného využití v praxi. Na jedné straně se mnoho potenciálních uživatelů nejen bojí skutečně elektronické identifikátory aplikovat, ale zároveň i ve výsledku vlastně neví, jak takový krok prakticky učinit a na druhé straně vystupují rozpaky mnoha společností v situacích, kdy jim je dokument opatřený elektronickým identifikátorem poskytnut a samy tyto organizace mnohokrát netuší, jak s ním nakládat. Právě pro usnadnění včlenění používání elektronických podpisů a elektronických pečetí do každodenního života a poskytnutí odpovědí na základní otázky jsem se rozhodla rozvést tuto problematiku ve své závěrečné práci ukončující pětileté studium na Právnické fakultě.

Pro pozvolný úvod do rozebírané problematiky jsem zasvětila úvodní kapitolu stručnému popisu historického vývoje elektronických identifikátorů. Podle mého názoru je vytvoření povědomí o procesu vzniku a následného progresu určitého fenoménu základem pro jeho následné důkladné pochopení. Například i studium na většině vysokých škol, Právnickou fakultu Univerzity Karlovy nevyjímaje, je zahájeno právě obecným úvodem obsahujícím i pojednání o historii a vývoji daného oboru. Chápání institutů soudobého práva by jistě bylo o mnoho komplikovanější, kdyby studenti nebyli nejdříve seznámeni se základy práva římského, z něhož celý náš právní systém ve své podstatě vychází. Stejně tak povědomí o historickém vývoji práva na našem území, a jeho ovlivňování systémy zahraničími, umožní pochopit zakotvení určitých současných právních institutů a jejich význam v platné legislativě.

V první kapitole jsem rozebrala nejen počátek technologií samotnou existenci elektronickou identifikaci a jejich použití umožňujících, ale i vývoj právní úpravy v rámci evropského práva a následně práva tuzemského, které v podstatě z první zmíněné úpravy samo vychází. Tato část tedy představuje nejen úvod k práci samotné, ale i pozvolné nastínění následně podrobněji rozebírané problematiky a seznámení čtenáře se základními používanými pojmy. Po jejím přečtení by měl být již připraven

poměrně snadno chápat vysvětlení základních typů elektronických identifikátorů rozebíraných v kapitole následující, vzhledem k tomu, že mu již bylo umožněno v dostatečném rozsahu do materie začít pronikat. Podle mého názoru se mi podařilo docílit záměru a v úvodní kapitole čtenáře nenásilně zasvětit do problematiky, se kterou se bude skrze celou práci setkávat a přinést mu základní přehled o ní.

Následující kapitola by se dala označit za těžiště a nejvýznamnější část celé diplomové práce. Pokusila jsem se v ní provést základní ucelený přehled všech typů elektronických identifikátorů používaných nejen v soukromoprávních poměrech, ale i ve vztahu s prvkem veřejnoprávním, a to z důvodu, aby byl poskytnut kompletní a ucelený soubor, který přinese čtenáři přehled o celé problematice. Rozebrala jsem i často používané chyby v terminologii, základní rozdíl mezi elektronickým a digitálním podpisem a upozornila na nedostatečnou právní úpravu dynamických biometrických podpisů, které ač se jejich používání stává stále více a více častějším, své zakotvení v zákonech stále postrádají. Pokud by se tento nedostatek podařilo napravit, mohla by tato skutečnost napomoci i ke zvýšení důvěryhodnosti tohoto nástroje a mohly by vymizet obavy, se kterými se stále často při předložení elektronického zařízení a speciálního pera osoby o provedení tohoto typu podpisu žádající, setkávají. Mě samotnou materie dynamických biometrických podpisů velmi zaujala a možná právě proto, že se jedná o nástroj pro mě jako laika v oblasti informačních technologií nejlépe uchopitelný a částečně pravděpodobně i díky minulé zkušenosti s tímto typem podpisu, se mi o nich psalo mnohonásobně jednodušeji, než o podpisech založených na systému duálních klíčů a případně i certifikátů. Druhá kapitola, domnívám se, naplňuje z největší části můj záměr, který jsem při počátku práce na tomto dokumentu stanovila a umožňuje vytvoření základní představy o základních typech elektronických identifikátorů.

Třetí část mé diplomové práce shrnuje technologické aspekty elektronických podpisů. Jedná se o část textu, která by měla být srozumitelná i pro naprostého laika v oblasti informačních technologií, kterému si však kladla za cíl poskytnout alespoň základní povědomí o fungování těchto instrumentů. Snažila jsem se proto popsat jednotlivé aspekty pouze do té hloubky, aby si čtenář dokázal vytvořit představu o tom, jak vše funguje z pohledu, který není tolik známý, ale na druhou stranu nezabíhat do všech podrobností, jimž by už osoba v oboru nezkušená nemusela naprosto správně porozumět a staly by se tak pouhým zatížením bez

jakéhokoliv výrazného přínosu. Z mého pohledu se jednalo o nejnáročnější část celé práce, vzhledem k tomu, že jsem sama byla v této oblasti naprostým amatérem a musela jsem přečíst množství vysvětlujících textů a absolvovat konzultace s osobami v tomto ohledu zkušenějšími. Na druhé straně i to byl jeden z cílů mého snažení. Chtěla jsem tvorbou diplomové práce obohatit nejen potenciálního čtenáře, ale vlastně i sama sebe, vzdělat se v dosud naprosto neznámém oboru a pokusit si zase o kousek rozšířit obzory. Nyní, po dopsání diplomové práce jsem přesvědčena o tom, že se mi podařilo stanoveného cíle dosáhnout a její třetí kapitola tvoří přesně takový celek, o jehož sestavení jsem usilovala.

Na závěr celého souboru jsem se rozhodla zařadit kapitolu, která bude ve své podstatě jakýmsi návodem k použití. Dospěla jsem k názoru, že teoretické popisování a vysvětlování v jistém ohledu neurčitých pojmů nemůže dokonale úspěšně napomoci k rozšíření používání elektronických identifikátorů a zbavení veřejnosti pochybností a obav z nich. Proto jsem se rozhodla, že součástí práce bude i část, která popíše fenomén z ryze praktického hlediska. Kam mají potenciální uživatelé vlastně zajít, co si připravit a co očekávat– základní praktické informace o probírané materii, které jsem považovala za vhodné zařadit. Myslím si, že jsem tyto aspekty rozebrala do dostatečných podrobností a vyřešila natolik, aby bylo zcela jasné, jak v konkrétních situacích postupovat. Závěrečnou část tedy mohu považovat za určité přiblížení práce praktické rovině a přenos dříve rozebíraných aspektů do běžného života. Jedná se tedy vlastně o dokonalý protiklad předchozí kapitoly, v níž byly rozebírány často velmi obtížně uchopitelný technické pojmy, které jsem dokonce ani já sama před započetím prací na tomto textu, nikdy neslyšela. Z ryze teoretické části, při jejímž pročítání si jen málo z nás umí vytvořit nějakou reálnou představu o probíraném textu, se následně uskutečnil přenos do situací každodenního života a zcela běžně užívaných termínů a nástrojů. Závěrečná kapitola je tedy vlastně aplikací veškeré dříve probírané teorie na praktické situace.

Po opětovném přečtení cílů diplomové práce vytyčených v jejím úvodu a uzavřeného textu sama hodnotím, že se mi podařilo stanoveného dosáhnout a naplnit tak všechny stanovené záměry. Práce shrnuje základní aspekty dané problematiky, provádí definici odborných pojmů a poskytuje i návod pro praktickou aplikaci všeho dříve teoreticky rozebraného. Kromě toho zdůrazňuje i mezery ve stávající právní úpravě a podněcuje k jejich vyplnění a zdokonalení. Dle mého zhodnocení se jedná o ucelený text, jenž materii obsahuje nejen v rovině teoretické, ale uskutečňuje i její

převod do ryze praktických životních situací. Nejedná se tedy o čistě akademický text určený pro odbornou zainteresovanou veřejnost, ale stejně tak se může stát i souborem, který bude schopen poměrně snadno uchopit i naprostý laik v oboru a osoba, která není zběhlá ani v právním odvětví, ani ve světě informačních technologií, avšak chce se dozvědět základní informace o elektronické identifikaci osob a text zákona nebo odborných příruček pro něj není bez obtíží srozumitelný. Věřím, že se mi tedy v předchozích řádcích podařilo splnit vše, co jsem si sama před jejich sepsáním stanovila a tato diplomová práce je přesně takovým souborem, jakým jsem ji chtěla učinit. Doufám, že ke stejnému závěru dojdou i další osoby, které si cestu tímto souborem samy projdou.

Seznam použitých zdrojů

1. Seznam použité literatury

Digesta, neboli, Pandekty: svazek I, kniha I-XV, vybrané části = Digesta, seu, Pandecta: tomus I, liber I-XV, fragmenta selecta. Přeložil Peter BLAHO, přeložil Jarmila BARTOŠÍKOVÁ, přeložil Michal SKŘEJPEK, přeložil Jakub ŽYTEK. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. Fontes iuris romani.

GERLOCH, Aleš. Teorie práva. 7. aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. Právnické učebnice (Aleš Čeněk).

DONÁT, Josef. Nařízení eIDAS: komentář. Praha: C. H. Beck, 2017. Beckovy komentáře.

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

2. Seznam použitých internetových zdrojů

S. Mason: Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation, In: SCRIPTed [online], 2012, 9:1, str. 82-103, str. 84, cit. [22. 4. 2018]. Dostupné na <http://script-ed.org/?p=327>.

Drucksache 14/4987. Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr. Deutscher Bundestag, 14. 12. 2000. str. 16-17, cit. [11. 6. 2018]. Dostupné z: http://dip21.bundestag.de/dip21/btd/14/049/1404987.pdf.

SignoSoft [online]. [cit. 1. 5, 2018]. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php

MGR. ING. KMENT, Vojtěch. Nahradí elektronický podpis prostý ten tradiční vlastnoruční?. *Bulletin advokacie* [online]. 2016, **2016** [cit. 10. 6. 2018]. Dostupné

z: http://www.bulletin-advokacie.cz/nahradi-elektronicky-podpis-prosty-ten-tradicni-vlastnorucni?browser=full.

Kdy je nově prostý elektronický podpis rovnocenný s podpisem vlastnoručním?. *Epravo* [online]. 2017, 12. 1. 2017 [cit. 18. 6. 2018]. Dostupné z: https://www.epravo.cz/top/clanky/kdy-je-nove-prosty-elektronicky-podpis-rovnocenny-s-podpisem-vlastnorucnim-104697.html.

SMEJKAL, Vladimír, KODL, Jindřich a Miroslav UŘIČAŘ. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*. [Online]. 2015, č. 11, s. 189. [cit. 20. 6. 2018]. Dostupné z: https://journals.muni.cz/revue/article/view/3586.

HARTL, Jan. Srovnání legislativy elektronického podpisu v ČR a v Německu. Praha, 2006. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce doc. Ing. Prokop Toman, CSc., [cit. 13. 6. 2018].

3. Seznam použitých právních předpisů

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

4. Seznam použité judikatury

Nález Ústavního soudu ze dne 1. 12. 1998, sp. zn. I. ÚS 41/98 (N 147/12 SbNU 363) s odkazem na usnesení Ústavního soudu ze dne 25. 11. 1993, sp. zn. II. ÚS 75/93 (U 3/2 SbNU 201).

5. Seznam ostatních zdrojů

Osobní konzultace s Ing. Janem Kellerem dne 10. 6. 2018, 14. 6. 2018, 18. 6. 2018.

Vlastní poznámky z přednášek prof. JUDr. Aleše Gerlocha, CSc. z předmětu Teorie práva I na Právnické fakultě Univerzity Karlovy

Seznam obrázků

Elektronická identifikace osob v soukromoprávních poměrech

Abstrakt

Diplomová práce se zabývá jednotlivými typy elektronických identifikátorů, které mohou v soukromoprávních poměrech používat jak fyzické, fyzické podnikající, tak právnické osoby. Jedná se o ucelený přehled všech těchto instrumentů, který se pokouší vyložit a shrnout velmi mladou a dosud ne příliš zažitou právní úpravu, která prozatím není v praxi rozsáhleji aplikována, proto je doplněna pouze jediným komentářem a postrádá i příslušnou judikaturu, jenž v mnoha případech napomůže výkladu a snazšímu pochopení problematiky. V práci jsou rozebrány nejen právní aspekty celé problematiky, ale text zabíhá i do technologických hledisek a snaží se i laikovi v oboru informačních technologií přiblížit základní principy fungování elektronických identifikátorů. Zároveň práce poskytuje jakýsi systematický návod potenciálním uživatelům těchto nástrojů, které by od jejich užívání mohla odradit například obava z jejich důvěryhodnosti a neznalost. Okrajově je zde rozebrána i historie vývoje elektronické identifikace, která ovšem není nijak zásadně dlouhá, vzhledem k tomu, že k rozvoji tohoto fenoménu došlo až zhruba v posledních sto letech. Důvodem, proč jsem si zvolila toto téma byla především snaha o to, aby má diplomová práce byla v jistém ohledu přínosem, nereferovala jen o problematice mnohokrát rozebrané a přinesla čtenáři nové poznatky spolu s osvětlením tématu, které je dosud pro většinu společnosti velkou neznámou. Po dokončení četby této práce by měl mít čtenář základní přehled o jednotlivých typech elektronické identifikace, jejich praktickém využití a možnostech, jak se může sám stát jejich uživatelem. Zároveň získá základní informace o skutečné technologii těchto nástrojů a nahlédne tak alespoň okrajově do oblasti, která není obecně tolik známá a v oblasti právnické odborné veřejnosti ne často rozebíraná. Seznámí se základními pojmy, jakými jsou například šifrování nebo elektronický otisk čili hash. V neposlední řadě by čtenáři měl být poskytnut zběžný přehled historického vývoje elektronické identifikace osob, který slouží především k lepšímu pochopení celé problematiky a utvoření základního přehledu, stejně tak jako u v podstatě u každého tématu.

Klíčová slova

elektronická identifikace, nařízení eIDAS, elektronický podpis, elektronická pečeť, kvalifikovaný certifikát, šifrování, hash

Electronic identification of persons in private law relationships

Abstract

This diploma thesis deals with the topic of electronic identification of persons in private law relationships. It defines all types of electronic identifiers, which can be used in private law relationships by both legal entities and so natural persons. This paper summarizes the young and not for long used legislations. This legislation is not often used in practice and for that reason it has the only commentary. The case law for this problematics is also lacking and that is why it could not be used as one of the sources, despite that it is in many cases one of the most used and valuable sources. This thesis analyses not only the legal aspects of the electronic identification, but also the technological aspects, which it tries to explain even to the readers, who can be absolutely untouched by the world of information technology. At the same time this diploma thesis provides instructions for potential users of instruments of electronic identification, who can be distrustful and insecure of its first time user experience. The minor part of this thesis deals with the history of electronic identification. This section is not extremely extensive due to the fact, that history of his phenomenon goes only about hundred years to the past. The main reason for choosing this subject for my final work was the intention to create a writing, that could be beneficial and not only resolves the problematics, which was dealt with many times in the past and does not give a real chance to discover something new and to this time unknown. After finishing the reading of this text the reader should be familiar with all types of electronic identification used in private law, its practical use and the ways how to become the user of them. Simultaneously he or she receives the information about the technological aspects of electronic identifiers and is given a possibility to discover the not the widely known facts, especially for the lawyers. The reader gets to know the terms, such as the encryption or hash. Last but not least he or she learns about the history or electronic identification, which can be useful to better understanding of whole subject matter.

Key words

electronic identification, eIDAS regulation, electronic signature, electronic seal, qualified certificate, encryption, hash