ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

TEZE K DIPLOMOVÉ PRÁCI

ELEKTRONICKÝ PODPIS V PRÁVNÍ ÚPRAVĚ A PRAXI

Jméno autora: Bc. Tomáš Hunal

Vedoucí diplomové práce: Mgr. Ivana Hájková

ELEKTRONICKÝ PODPIS V PRÁVNÍ ÚPRAVĚ A PRAXI

1. Úvod

Podepisování samo o sobě je velmi důležitým aktem v životě každého jedince. V jako takovém jde o posloupnost znaků, které identifikují podepisující osobu. Vlastnoruční podpis splňující požadavky Občanského zákoníku má signifikatní právní váhu. Umožňuje prokázat jednoznačné spojení podepisující osoby a podepsaného dokumentu. Ovšem nejvyšší právní váhu má vlastnoruční podpis ověřený např. notářem. Takto ověřený podpis je vyžadován v celé řadě právních případů a plní i tzv. legalizační funkci. Všechny tyto aspekty bere v úvahu i (zaručený) podpis elektronický.

2. Cíle a metodika

Hlavním cílem diplomové práce je popsat problematiku elektronického podpisu, a to z mnoha hledisek. To znamená vyjít z prozkoumání legislativy v České republice v návaznosti na normy platné v EU či závěry vytvořené v rámci OSN. Dalším cílem je popsat stylem srozumitelným i laikům princip elektronického podpisu s využitím poznatků z kryptologie a příbuzných odvětví, popsat na příkladu jeho aplikaci. Pochopitelně jednou ze stěžejních částí by měla být pasáž od praktických možnostech používání a také o jeho skutečném využití v praxi. Metodicky je prvním krokem je vyhledání, prostudování a popis platné právní úpravy, tj. zákona č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů ze dne 29. června 2000 ve znění pozdějších novelizací, a souvisejících legislativních úprav (vyhláška Úřadu na ochranu osobních údajů; nařízení vlády; standardy vydávané ÚOOÚ). Vyžaduje to studium dostupných zdrojů v knihovnách, resp. vyhledávání informací na internetu. Protože mi není známo, že by pro tuto problematiku byl k dispozici skutečně komplexní výkladový pramen, budu vycházet zejména z prostudovaných materiálů a pochopitelně odborných konzultací.

3. Technologie elektronického podpisu

Podle zákona 227/2000 Sb. ve znění pozdějších novelizací se elektronickým podpisem rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě, nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Zaručeným elektronickým podpisem je pak elektronický podpis, který je jednoznačně spojen s podepisující osobou, který umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, který byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou a je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. Podepsáno může být v podstatě cokoliv, a to i bez vytištění na papír. Cokoliv znamená třeba i obsah diskety, fotografie, přístupy k webovým serverům, emailová zpráva apod. K hlavním principům elektronického podpisu patří:

- *Autentičnost* - potvrzení, že zpráva skutečně pochází od toho, kdo se vydává za jejího autora.
- *Integrita* - sebemenší změna toho, co je podepsáno, způsobuje i změnu samotného podpisu. Pokud by tedy někdo změnil sebemenší maličkost na již jednou podepsaném dokumentu, bude to okamžitě patrné.
- *Nepopiratelnost* - neumožňuje nikomu při konfrontaci s podepsaným dokumentem říci něco ve smyslu: „já jsem nic takového nepodepsal, to musí být podvrh.“ Lze totiž věrohodně prokázat, že podpis nemohl vytvořit nikdo jiný - takže autor nemůže své autorství později popřít.

Nicméně z výše uvedeného vyplývá, že elektronickým podpisem by mohl být řetězec bitů (např. naskenovaný podpis) pod e-mailem. Zde však bude díky schopnosti výpočetní techniky obtížné dokázat, zda se naskenovaný podpis ocitl na dokumentu z vůle uvedené osoby. Tyto problémy odstraňuje až zaručený elektronický podpis. Základním rozdílem mezi nimi je skutečnost, že zaručený elektronický podpis dle § 2 písm. b) umožňuje **identifikaci** podepisující osoby (ve vztahu k datové zprávě). Kdežto „obyčejný“ elektronický podpis umožňuje **ověření totožnosti** podepsané osoby vzhledem k podepsané zprávě. Jestliže tedy zákon 227/2000 Sb. říká, že EP „umožňuje ověření totožnosti podepsané osoby vzhledem k datové zprávě“, nemyslí se tím, že elektronickým podpisem je toto „*ověření*“ také už

automaticky vykonáno. Zákon jen říká, že je to „umožněno“, tj. že EP může napomoci k tomu, aby si příjemce totožnost podepsané osoby ověřil, ale nijak výsledek tohoto ověření nezaručuje. Pokud například pod e-mailem bude uveden text „Petr Novák, Na Vyhlídce 13, Praha“, je to právě případ EP, neboť dává možnost (cestu) k ověření totožnosti[1] . V případě, že je ke zprávě přiložen zaručený elektronický podpis, založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření podpisu, je to jako kdyby podpis Petra Nováka pod touto zprávou ověřil už přímo notář, tedy toto „*ověření*“ je už automaticky vykonáno.

Zásadní je tedy ověřitelnost elektronického podpisu ve vztahu k autorovi. Proto byl vytvořen tzv. digitální podpis, který umožňuje jednoznačnou identifikaci osoby. Digitální podpis je v podstatě spojením klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka. Certifikát je pak vydáván třetí nezávislou osobou (certifikační autorita), která tak stvrzuje jeho pravost. Je potřeba rozlišit v této souvislosti i certifikáty. Český zákon vyžaduje pro komunikaci občana s orgány veřejné moci certifikát kvalifikovaný, vydaný akreditovaným poskytovatelem certifikačních služeb (pro jiné využití tedy není potřeba kvalifikovaný certifikát, ale „postačuje obyčejný“ certifikát od jakékoliv certifikační autority jež si strany navzájem uznají za důvěryhodnou). Certifikační autorita tedy vydá občanovi elektronický certifikát na bázi asymetrické kryptografie. To je kryptografická technika pro šifrování dat a digitální podpisy, která používá dvojice klíčů. Jeden z klíčů slouží k šifrování dat či k digitálnímu podpisu a druhý k dešifrování dat či k ověření pravosti digitálního podpisu. Pouze jeden z klíčů (soukromý klíč) se uchovává v tajnosti, zatímco druhý klíč (veřejný klíč) se zveřejňuje pomocí papírových a elektronických médií. Princip spočívá v tom, že pomocí veřejného klíče lze ověřit pravost klíče soukromého, ale přesto nelze z veřejného klíče odvodit klíč soukromý! Soukromý (privátní, tajný) klíč jsou jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu a (nebo) k dešifrování dat. Musí být uchováván v tajnosti a jeho znalost přísluší pouze jeho vlastníku. Samotný zákon ukládá vlastníku soukromého klíče (podepisující osobě) povinnost zacházet s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití

[1] SMEJKAL, V. *Otázky, otázky*…. E-podpisy [online], 2002, [cit. 2002-04-05]. Dostupný z: <http://www.e-podpisy.cz/index.php?template=faq.html>.

Na straně podepisující osoby se z napsané zprávy pomocí hashovací funkce vytvoří tzv. otisk zprávy (HASH 1). Na vstupu hashovací funkce může být libovolná a libovolně dlouhá datová zpráva, na jejím výstupu je však otisk, který má pevnou délku 128 nebo 160 bitů (první údaj platí pro hashovací funkci MD5, druhý pro SHA-1). Pokud by podepisující osoba ve zprávě změnila byť jediné písmeno, na výstupu získá zcela jiný otisk. Otisk napsané zprávy se šifruje za pomoci zvoleného asymetrického algoritmu a pomocí soukromého klíče osoby, která se podepisuje. Získaný výsledek je digitálním podpisem, který je ke zprávě připojen. Na straně příjemce zprávy se k otevřenému textu vypočte hash (HASH 2). Z digitálního podpisu se pomocí veřejného klíče osoby, která zprávu podepsala, získá hodnota, která by se měla rovnat hodnotě HASH 1. Pokud jsou hodnoty HASH 1 a HASH 2 shodné, má příjemce jistotu, že zpráva nebyla cestou změněna a že zprávu podepsala daná osoba svým soukromým klíčem.

4. Elektronický podpis v praxi

Podle mého názoru lze rozdělit možnost praktického využívání elektronického podpisu do třech v současné době primárních oblastí využití. Jedná se o:

1. bankovnictví,
2. elektronické obchodování,
3. veřejnou správu a samosprávu.

4.1 Elektronické bankovnictví

Klient uzavře s bankovním ústavem smlouvu o zřízení elektronického bankovnictví (přesný název se u jednotlivých bank liší). Banka při podpisu smlouvy vydá klientovi instalační software (obvykle ve formě CD - ROM). Klient doma, na svém počítači, který musí mít určitou minimální konfiguraci (velikost RAM, volné místo na harddisku, operační systém, rychlost procesoru, připojení na internet) vygenereruje elektronické klíče (viz soukromý a veřejný klíč). Před první elektronickou komunikací s bankou je třeba předat veřejnou část elektronického klíče do banky. Klient například musí do banky přinést disketu s veřejnou částí elektronického klíče, aby banka mohla kontrolovat platnost elektronických podpisů dávek přijatých od klienta. Za bezpečný způsob podepisování (který se v současné době rychle rozšiřuje) lze považovat uložení soukromého klíče nezbytného pro podepsání aktivních

transakcí (tj. příkaz k úhradě, zadání trvalého platebního příkazu, atp.) na čipovou kartu, kterou soukromý klíč nikdy neopustí a nelze jej zkopírovat (návdavkem je použití soukromého klíče chráněno PINem). Ovšem „nevýhodou“ se může zdát nutnost vybavení počítače čtečkou čipových karet, jejichž ceny se pohybují od 1500 Kč výše.

4.2 Elektronické obchodování

Elektronické obchodování představuje širokou oblast využití elektronického podpisu. Je to jednak oblast vztahu zákazník (spotřebitel) - prodejce, a tedy v podstatě nákup po internetu. Druhou oblastí jsou klasické kontakty mezi obchodními partnery, jako jsou různé faktury, objednávky, potvrzení, výběrová řízení atp. Elektronický podpis zde dává jistotu, že zákazník stejně jako obchodník budou mít záruku, že člověk, se kterým obchodují a kterého třeba nikdy osobně neuvidí, je existujícím partnerem. Stejně tak poskytuje garanci, že zprávy, dokumenty a faktury dopravované po komunikačních sítích nebyly cestou změněny a že jejich autorem je skutečně jejich obchodní partner.

4.3 Elektronický podpis a veřejná správa

Z textu zákona č. 227/2000 Sb. vyplývá, že pro tyto druhy komunikace (v oblasti orgánů veřejné moci) je vyžadován podle § 11 zákona zaručený elektronický podpis založený na kvalifikovaném certifikátu vydávaný akreditovanými poskytovateli certifikačních služeb. V současné době je Ministerstvem informatiky akreditována pouze jedna společnost. Celým procesem akreditace prošla zatím pouze 1.CA (neboli první certifikační autorita). Aby mohly orgány veřejné moci vůbec elektronicky podepsaná podání přijímat, musely být učiněny určité kroky. Takovým krokem bylo vydání Nařízení vlády č. 304/2001 z 25. července 2001 o zřízení elektronických podatelen. Tato pracoviště pro příjem a odesílání datových zpráv musí být vybavena potřebnými zařízeními připojenými k veřejné datové síti a budou muset splňovat požadavky na technické a programové vybavení podle standardů Úřadu pro veřejné informační systémy.

V současné době již existují první projekty, kde je možné využívat elektronického podpisu ve styku s orgány veřejné moci. Lze elektronicky žádat o dávky Státní sociální podpory, lze podat přiznání k dani z přidané hodnoty, komunikovat s celní správou nebo úřadem ombudsmana apod. Je však na mnoha místech stále ještě nutné překonávat určitou psychologickou bariéru, neboť stále existují lidé, a i úředníci jsou jen lidé, kteří elektronickému podpisu nedůvěřují. Pouze lidé, kteří dobře porozumí podstatě elektronického podpisu, zejména zaručeného elektronického podpisu, ho budou ochotni používat. Navíc se mnoho lidí nedokáže vyrovnat s opuštěním papíru jakožto jediného úředního nosiče a „mít to černé na bílém!".

5. Závěr

Jsem hluboce přesvědčen, že elektronický podpis má budoucnost. Pro mnohé předběhl svoji dobu, ale dříve nebo později bude adoptován a široce využíván. Musí překonat počáteční skepsi i přirozenou nedůvěru k novým „věcem", určitě dojde k jeho zlevnění a tím také k rozšíření možností jeho využití. Známý latinský citát říká: *„VOX AUDITA PERIT, LITTERA SCRIPTA MANET"*, tedy „pomíjí slyšený hlas, trvá napsané slovo". Já si jen přeji, abychom za napsané slovo již brzy automaticky považovali i slovo v podobě elektronické a pomyslně tak dokončili cestu k informační společnosti.