

Zákon o elektronickém podpisu

Vznik společné evropské měny umožnil to, co ve Spojených státech probíhá již několik let – až neskutečný růst elektronického obchodu. Evropa v tomto trendu dosud značně zaostávala. Ukazuje se, že hlavním důvodem bylo právě měnové rozdělení regionu na poměrně malé oblasti. V této situaci tedy zbývá pouze jediné. Na úrovni jednotlivých zemí zakotvit pojem elektronického podpisu, který umožní bezpečné uskutečňování obchodních transakcí.

Abyste mohli sami posoudit kvalitu návrhu zákona o elektronickém podpisu, případně pravdivost toho, co vám o tom chci sám říci, tak je potřeba udělat malý úvod do veřejné kryptografie. Podrobnější informace naleznete v čísle 5/99.

Co znamená pojem elektronický podpis

Jestliže se na pojem elektronický (nebo také digitální) podpis podíváme z pohledu práva, tak je to obdoba klasického podpisu, nebo razítka tak, jak je znáte z běžné praxe s tím, že neslouží k podepsání (autentizaci) papírových, ale elektronických dokumentů.

Bohužel elektronické dokumenty mají trochu jiné vlastnosti, než dokumenty listinné. Základním rozdílem je **snadnost kopírování elektronických dokumentů**. Mnoho lidí si vytváří archívy obrázků pro vlastní potěšení a podle vlastních zájmů. V drtivé většině jsou to archívy elektronické. Nechci se dotýkat vaší ekonomické situace, ale vytvořit elektronickou kopii čehokoliv je nesrovnatelně levnější, než to samé udělat na papíře (o kvalitě ani nemluvě).

Intuitivní elektronický podpis

Většina lidí, jestliže slyší „elektronický podpis“, tak si představí následující postup. Vytvořím listinu, podepíši ji, naskenuji a pošlu jako soubor. Příjemce si ji vytiskne a výsledek je vlastně stejný (jestliže mám kvalitní tiskárnu a skener).

Toto je ale zásadní omyl. Jestliže kdokoli získá elektronický obraz vašeho podpisu, tak pro něj většinou není problém jej z dokumentu vyjmout, očistit od pozadí (jestli tam nějaké je) a posléze přidat k čemu on bude chtít. Možná si myslíte, že s listinami je možné dělat to samé. Bohužel jsou zde zásadní rozdíly: cena, kvalita a nebezpečnost. Při práci s listinou se ji nejdříve musíte zmocnit, musíte se setkat s lidmi, kteří pro vás vytvoří padělek, musíte padělanou listinu nějak doručit příjemci, atd. Při použití elektronických dokumentů lze všechny tyto činnosti velmi snadno a levně provést anonymně. A navíc, jak bychom vyřešili problém podpisu dokumentů, které již jako elektronické vznikají?

Takže kopie dokumentů fungovat nebude a jestliže se mluví o elektronickém podpisu, tak nejde o obrázek, což vám řeknou všichni odborníci.

Skutečný elektronický podpis

Pojem elektronický podpis pochází z vědy, které se říká kryptografie a byl objeven v roce 1976, nejdříve jako teoretický koncept, první praktický postup pro jeho vytváření byl objeven v roce 1977. Elektronický podpis je součástí veřejné kryptografie – jedné ze základních oblastí moderní kryptografie. Jestliže někdo tvrdí (což dále uvidíme), že chce elektronický podpis definovat ještě obecněji, tak to svědčí pouze o jednom, že prostě nerozumí základním myšlenkám dané oblasti.

Jak tedy elektronický podpis teoreticky funguje? Velmi stručně:

1. je třeba **vytvořit prostředky pro vytváření a ověřování elektronického podpisu**. Těmto prostředkům se říká klíč a skládá se ze dvou částí – veřejné a soukromé.
2. vytvářím podpis - **podepisuji**. Potřebujeme zprávu a soukromý klíč (podepisuji, nikoliv šifruji). Podpis si můžeme představit jako elektronickou zprávu, která má přesně stanovenou (malou) délku, která nezávisí na délce podepisované zprávy.
3. **ověřuji podpis**. Zde potřebujeme zprávu, podpis a veřejný klíč. Výsledek je jednoznačný a správný – ano/ne.

Podpis listiny vs. elektronický podpis

Nyní se můžeme pokusit najít analogie mezi zmiňovanými dvěma typy podpisu.

Pojem	Listina	Elektronická zpráva
Zpráva	listina	data v elektronickém tvaru

Podpis	„čmáranice“ vytvořená lidskou rukou	Elektronická zpráva vytvořená na základě veřejné kryptografie
Prostředek pro vytvoření podpisu	schopnost mozku, cvik, schopnost ruky, apod.	Soukromý klíč
Prostředek pro ověření podpisu	znalosti, zkušenosti, schopnost lidského oka, podpisový vzor	Certifikát veřejného klíče

Jak vidíte, tak pro ověření klasického podpisu je potřeba mimo jiné podpisového vzoru. Co takový podpisový vzor vlastně obsahuje? Je tam jméno dané osoby, její adresa, číslo občanského průkazu, rodné číslo a samozřejmě podpis. Dá se tedy říci, že ve chvíli, kdy najdeme podpisový vzor odpovídající ověřovanému podpisu, tak získáme i pravděpodobnou identitu osoby, které ten daný podpis patří. Jak je to ale s elektronickým podpisem. Kde se tam skrývá toto propojení podpis-osoba?

Nalezení odpovědi na tuto otázku znamená vyřešení fundamentálního problému veřejné kryptografie! Zároveň je to i důvod, proč vůbec musí vzniknout něco jako zákon o elektronickém podpisu. Vůbec nejde o to, jak vytvořit elektronický podpis. Postupy pro toto jsou známy a široce se používají. Problémem, který je třeba vyřešit je právě zajištění důvěryhodné vazby mezi veřejným klíčem a osobou.

Tím se dostáváme k pojmu **certifikát veřejného klíče**, což je další pojem, který je třeba vysvětlit před tím, než se podíváme na návrhy českých zákonů o elektronickém podpisu.

Certifikát veřejného klíče

Základním problémem je tedy, jak jsme si řekli dříve, propojit osobu a veřejný klíč. Na řešení tohoto zadání vznikly dva přístupy.

PGP

První je založen na vzájemné důvěře (systém PGP), kdy já mám veřejné klíče mých přátel a ty předám dalším přátelům, čímž vznikají tzv. keyrings. Systém je to velmi jednoduchý, má ovšem své mouchy. Jednak teoretické (neexistuje žádná pevná záruka, že PGP klíč Daniela Cvrčka je opravdu klíč Daniela Cvrčka, protože pro bezpečné předání je potřeba fyzický kontakt s vlastníkem klíče, což lze málokdy v praxi splnit), a jednak praktické, vážící se na implementaci. Ukazuje se, že náhodná čísla v programu PGP nejsou zase až tak moc náhodná. Jistý člověk si z webové stránky Bílého domu stáhl PGP klíč Billa Clintona. Pak spustil vyhledávání tohoto klíče na všech velkých serverech s PGP klíči ve Spojených státech. Jaké bylo jeho překvapení, když našel další 63 osob, které měly stejný veřejný klíč. V praxi to znamená, že těchto 63 osob mělo zákonitě i stejný soukromý klíč, takže kterákoliv z těchto osob mohla podepisovat elektronické dokumenty jak Bill Clinton.

X.509

To co má budoucnost (oficiální) jsou systémy založené na normě X.509. Základní myšlenkou tohoto systému je vznik **certifikačních autorit**, které jsou důvěryhodnými centry. Tato centra se starají o zveřejňování veřejných klíčů svých zákazníků tak, aby jim bylo možno věřit. Pro to používají **certifikátů veřejných klíčů**, které obsahují např. identifikaci vlastníka, veřejný klíč a jeho platnost a identifikaci certifikační autority. Tyto údaje jsou certifikační autoritou podepsány (autentizovány).

Certifikační autority

Bylo by nebezpečné a nepraktické, abychom měli jednu certifikační autoritu pro celou zemi. Proto je možno vytvářet tzv. stromy certifikačních autorit. Kořenová certifikační autorita (např. pro EU) vytvoří certifikát pro certifikační autority jednotlivých členských zemí. Ty zase vytvoří certifikáty pro certifikační autority na úrovni krajů, atd. Jestliže potom bezpečně získáte veřejný klíč kořenové certifikační autority, tak je možné plně automaticky ověřit platnost certifikátů, a tím i konkrétních podpisů, vytvořených v celé Evropské unii.

Návrh zákona o elektronickém podpisu

V současné době (začátek října) existují dva návrhy zákona o elektronickém podpisu. První z nich (vládní) je vytvářen už více než rok. První návrhy opravdu „stály“ za to. Naštěstí výroky typu: „certifikát veřejného klíče je listina“ byly postupem času odhozeny na smetiště dějin. V kostce se dá říci, že rok práce je znát a totální nesmysly se

tam už najít nedají. Na druhou stranu k poslední verzi, kterou jsem měl možnost číst a která byla z počátku září se dá napsat celkem slušný seznam připomínek. Bohužel neměl jsem možnost dostat se k poslední verzi, takže se tímto nechci dále zabývat. Můj vlastní názor je asi takový, že návrh není ideální, ale neobsahuje vyložené nesmysly. Čím se chci zabývat podrobněji je zákon, který předložil SPIS (Sdružení pro informační společnost) v čele s panem Smejkaem. Nevím, jak dlouho na tomto návrhu pracovali, ani nevím kdo přesně, ale když jsem si ho poprvé přečetl, tak jsem si myslel, že to ani nemůže být pravda. Abych podpořil tento svůj názor, tak se pokusme projít důvodovou zprávu k tomuto základu, která poskytuje i určitý pohled na záměr, který jeho autoři mají. Začneme od začátku.

K §2 Základní pojmy

Pojmy v tomto paragrafu definované mají vycházet z dokumentů EU a OSN. Bohužel, autoři asi nenašli dost síly k tomu, aby alespoň přeložili pojmy v těchto dokumentech definované, což vede k obrovským problémům v prakticky celém návrhu zákona. Navíc to, co přeložili, přeložili značně nešťastně.

Odstavec 2

Jestliže porovnáme definici pojmu elektronický podpis s definicí z dokumentu *Directive of the European Parliament and of the Council on a common framework for electronic signatures*, tak zjistíme, že věta

elektronický podpis je vytvořen prostředky, které podpisovatel může udržet pod svou výlučnou kontrolou“ byl nahrazen spojením

„elektronický podpis ...byl vytvořen a připojen k datové zprávě způsoby, které jsou pod kontrolou oprávněné osoby ”.

To je značně nepřesný překlad a slovo *způsoby* zahrnuje např. postup jak to provést, který je (a musí být) všeobecně znám, ale neobsahuje již např. soukromý klíč, kterýžto pojem nezbytně obsahovat musí. Kromě toho je vynechána poslední část definice elektronického podpisu a totiž, že

...elektronický podpis je k datům připojen takovým způsobem, že jakákoliv jejich změna je zjistitelná.

Můžete říci, že to je hra se slovíčky. Potom ovšem následující zdůvodnění podané definice je naprosto nesmyslné.

„...technologicky nezávislá formulace navrhovaného zákona umožňuje využití i jiných, doposud pouze teoreticky uvažovaných metod identifikace osob (např. vzorců DNA, snímků duhovky oka, otisku prstů apod.).“

Jestliže jste četli předchozí úvod k elektronickému podpisu, tak si jistě pamatujete, že tzv. veřejná kryptografie (nejde o technologii, ale o matematickou definici) umožnila vznik elektronického podpisu a je jeho nutným předpokladem. Jestliže chci elektronicky podepisovat dokumenty, tak potřebuji nějaké tajemství, což nevím kde chtějí autoři např. u otisku prstu, nebo u DNA najít. A za druhé, prostředky pro elektronický podpis nemohou sloužit k identifikaci osoby. To je **absolutní nepochopení základních principů** oblasti elektronických podpisů.

Odstavec 4

Ten je naprosto jasný a nepřipouští pochybnosti. Je třeba vytvořit úřad a ten musí mít předsedu. Navíc tento úřad má být vytvořen při Ministerstvu dopravy a spojů. Neslyšel jsem o žádných odbornících, kteří by na zmiňovaném úřadu pracovali..., nebo že by měl přijít někdo zvenčí?

Počínaje odstavcem 5 začíná základní nedorozumění kdy místo správného pojmu „prostředek pro vytvoření elektronického podpisu“ je použit pojem elektronický podpis.

Odstavec 6

Zde je definován zcela „originální“ pojem ověřovatel informací. Přitom ve všech dokumentech, které jsem kdy četl se používá pojem certifikační autority, případně poskytovatel certifikačních služeb. Zavedený pojem totiž vytváří dojem, že daný subjekt něco ověřuje, což není úplně pravda. Daný subjekt vytváří (mimo jiné) certifikáty veřejných klíčů, přičemž jednou ze součástí této činnosti je ověření identity subjektu, který žádá o vytvoření certifikátu veřejného klíče. Je zajímavé, že ačkoliv se o několik řádků výše mluví o obecnosti, tak se zde snaží vyjmenovat konkrétní informace zajišťující jednoznačnou identifikaci konkrétní osoby.

Konečně certifikát veřejného klíče je zde nezvykle nazván ověřením!?!

K §3

Odstavec 2 je velmi zajímavý.

„Zaručený elektronický podpis zaručuje, že datovou zprávu podepsala oprávněná osoba. ...“

Je to sice pěkné tvrzení, ale obávám se, že u soudu by neobstálo. Elektronický podpis totiž nic takového automaticky nezaručuje. Představte si třeba situaci, kdy odjedete na měsíc na dovolenou. Po příjezdu zjistíte, že se vám někdo vloupal do kanceláře a dostal se k datům z vašeho počítače (pokud je to ovšem vůbec možné zjistit). Okamžitě se spojte s certifikační autoritou a oznámte ji, že chcete odvolat všechny své certifikáty veřejných klíčů. Co ovšem

s dokumenty, které byly v mezidobí vytvořeny a „vámi“ podepsány? Uzná je soud, nebo neuzná? Je to problém, protože situace může být i opačná. Vy vytvoříte dokument, kterým se k něčemu zavázete, ale po nějaké době zjistíte, že se vám to už nelíbí. Nahlásíte tedy certifikační autoritě, aby odvolala vaše certifikáty.

Jak vidíte, tak to není vůbec jednoduchý problém. Řešením jsou v současné době tzv. poskytovatelé notářských služeb. Jestliže si chcete být jisti, tak vám notář vystaví potvrzení o vytvoření zprávy a současně tuto akci uloží do svého archívu. Jestliže dojde ke sporu, tak může vystupovat jako nezávislá osoba. Bohužel, tento pojem není vůbec zaváděn (a to nejen u nás).

K §4

Definuje další vlastnosti elektronického podpisu, který nebyl definován v §2. Proč zde, to nevím.

K §5

Kromě toho, že zaručený elektronický podpis byl definován v §2 to není zase až tak úplně nesmyslné. Tedy až na následující:

„Zaručený elektronický podpis ...je chráněn proti padělení dostupnými technologiemi a může být spolehlivě chráněn podepsanou osobou před použitím jakoukoliv jinou osobou“.

Co to je padělení elektronické informace??? Vždy jsem si myslel, že padělení je vytváření nepovolených kopií. Jak ovšem u elektronické informace poznáte originál od kopie? A navíc, čemu to vůbec může uškodit? Vždyť jestliže není elektronický podpis spojen s konkrétní zprávou a konkrétním autorem, tak je naprosto bezcenný!

Co to znamená, že podpis může být spolehlivě chráněn podepsanou osobou? Vždyť celý koncept elektronického podpisu byl vytvořen proto, aby bylo možno bezpečně přenášet data v prostředí, které není bezpečné a nad kterým nemáme moc!

K §7

Jestliže si přečtete tento paragraf, tak už opravdu nabýváte dojmu, že buď není rozdíl mezi podpisem a prostředkem pro vytvoření podpisu (soukromý klíč), nebo si autoři tyto dva pojmy spletli.

„1. Oprávněná osoba je povinna:

- a) **nakládat s elektronickým podpisem s náležitou péčí tak, aby nemohlo dojít k jeho neoprávněnému použití;**
- b) **uvědomit neprodleně ověřovatele informace v případě, že hrozí nebezpečí zneužití jeho zaručeného elektronického podpisu;**
- c) **zajistit, aby všechny informace, které se jí týkají ve vztahu k zaručenému elektronickému podpisu, jež sdělí ověřovateli informace nebo jiným subjektům, byly přesné, pravdivé a úplné.“**

První dvě písmena by byla srozumitelná právě tehdy, kdyby byl použit pojem prostředkem pro vytváření elektronického podpisu. Písmeno c) už pro mě není pochopitelné vůbec.

K §8

S paragrafem 8 lze v zásadě souhlasit, ovšem zdá se mi poněkud chudý. Chybějí mi tam následující body:

1. Certifikační autorita je povinna zajistit, že žadatel o certifikát vlastní prostředky pro vytváření elektronického podpisu. (Je třeba prokázat vlastnictví soukromého klíče. Jinak bych si mohl nechat vytvořit certifikát na své jméno s veřejným klíčem kohokoliv jiného.)
2. Jestliže certifikační autorita generuje i soukromý klíč pro zákazníka, tak je povinna se ujistit, že zákazník je schopen použít jak prostředky pro vytváření, tak i pro ověřování elektronického podpisu.
3. Certifikační autorita je povinna zveřejnit informace o možném zneužití prostředků pro vytváření elektronického podpisu.
4. Uchovávat informace o všem činnostech, které kdy provedla (vytváření certifikátů, odvolávání certifikátů, ...).
5. ...

Určitou zajímavostí je, že se zde vyskytuje pojem certifikát. Nikde jinde použit není a je zajímavé, že není ani nikde definován!

K §9

Tento paragraf je asi v pořádku (nejsem právník, takže to nedokáži přesně určit), ale nechápu jej. Jak může platit ochrana osobních údajů, když informace, které osoby sdělí certifikační autoritě jsou součástí certifikátu veřejného

klíče, který je veřejně přístupný. Něco jiného jsou ovšem listinné dokumenty, které byly použity při ověřování totožnosti dané osoby.

§10 Úřad

Tento paragraf se věnuje činnostem Úřadu a při jeho stručnosti mu nelze asi nic vytknout.

§11 Ověřovatel informací

Toto je opět paragraf, ke kterému se nemohu nějak moc vyjadřovat, jelikož k tomu nemám potřebné znalosti. Zajímavý je z mého pohledu pouze odstavec 6.

„Kromě činností uvedených v tomto zákoně může ověřovatel informací bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec.“

Cílem je (naprosto správně) zajistit, aby se certifikační autorita (ověřovatel informací) nemohl věnovat činnostem, které bezprostředně nesouvisí s činnostmi podle tohoto zákona. Dobrým důvodem pro toto je konflikt zájmů.

§12 Osvědčení o zaručeném elektronickém podpisu

Osvědčení o podpisu je sám o sobě originální pojem. Zdá se, že jsme opět jedineční a žije v nás tradice bratří Čapků, kteří byly ovšem ve vytváření nových pojmů, zdá se mi, úspěšnější.

Jsou zde definovány věci, které mi chyběly v §8, kde by bylo jejich umístění logičtější.

Trochu měl zarazit odstavec 10, který říká, že:

„Technické komponenty, které může ověřovatel informací používat k výkonu své činnosti, stanoví Ministerstvo dopravy a spojů vyhláškou.“

Zdá se mi, že jde až o přílišnou pravomoc, kterou by měl neviditelný úředník. Podle mého názoru by umožňoval např. definovat programové balíky, které lze používat a které ne, jaké používat počítače, atd. Tato formulace se mi nezdá příliš dobrá.

§13 Obsah osvědčení

K tomuto paragrafu má pouze dvě připomínky. Za prvé, prostředek pro ověření elektronického podpisu je nazýván **„datovou zprávou sloužící k ověření elektronického podpisu“**, což není až tak špatné, ale každopádně je z toho cítit snaha o vlastní, nepřilíš přesné názvosloví. Druhá připomínka se týká odstavce 2.

„Další údaje smí osvědčení obsahovat jen se svolením oprávněné osoby.“

Motivace pochází z ochrany osobních údajů, bohužel ovšem omezuje možnosti certifikační autority vložit do certifikátu (o ten tady jde, i když se mu říká jinak) údaje, které definuje ve vlastních prováděcích předpisech a které mohou být nepostradatelné pro její další činnosti.

§14 Povinnosti ověřovatele při ukončení činnosti

Tento paragraf je podle mého názoru dosti problematický. Popisuje, že při ukončení činnosti certifikační autority přejímá její povinnosti (správu všech certifikátů) jiná certifikační autorita. Tento postup se mi nezdá vhodný z několika důvodů. Dva základní jsou následující:

1. Ochrana osobních údajů – certifikační autorita je pouze správcem osobních údajů svých klientů a není možné, aby je podle vlastního uvážení komukoliv předávala.
2. Na prostředky pro vytváření elektronických podpisů (soukromé klíče) certifikační autority jsou kladeny ty nejvyšší možné bezpečnostní požadavky. Obávám se, že by bylo velmi obtížné tyto požadavky splnit v případě, kdy by měli být předány úplně cizímu subjektu. Kdo by za ně měl následně odpovědnost? Nový „vlastník“, nebo předchozí certifikační autorita, která již sice právně neexistuje, ale dané prostředky může nadále vlastnit, čemuž se technicky nedá zabránit.

Mnohem vhodnější je případně finanční vypořádání certifikační autority se svými klienty (vrácení peněz za neuskutečněné dohodnutých služeb) s tím, že klienti sami se rozhodnou, služeb které certifikační autority budou nadále využívat.

§16 Zrušení osvědčení

Důvody pro zmiňovanou akci jsou jasné. Chybí mi zde postih certifikační autority, jestliže je původcem problémů. Co zde také postrádám je možnost pozastavení platnosti certifikátů. To je prostředek vhodný např. při dočasném přerušení vytváření elektronických podpisů (např. zmiňovaná dovolená).

Paragrafy 17 a 19 se týkají uznávání zahraničních osvědčení a pokut a nemám jim co vytknout. Zajímavý je ovšem paragraf 18. Chybí mi zde návaznost na certifikaci programového vybavení, jejíž prováděcí předpisy již existují v rámci NBÚ. Dále tvrzení:

„Technické a programové komponenty, které umožní ověřovat nebo vytvořit zaručený elektronický podpis, musí v sobě zahrnovat taková bezpečnostní opatření, aby nemohlo dojít k jeho zneužití.“

Není dobře definované. Zneužití můžeme ztížit, nikoliv ovšem zabránit. K tomu je nutno definovat např. fyzickou ochranu zařízení, či administrativní opatření.

Závěrem

Udivujeme mě, pod jaký dokument dal pan Smejkal svůj podpis. Vzhledem k tomu, jak často je vidět ve sdělovacích prostředcích a jaký vliv má společnost, jejímž je předsedou, tak mne tento jeho počín opravdu ohromuje. Návrh zákona, který zaštitily čtyři politické strany vykazuje základní nedostatky, zmatení pojmů, neúplnost. I když nemám nijak rád současnou vládu, tak musím říci, že vládní návrh (předkládaný Úřadem pro státní informační systém) je neporovnatelně lepší.

Názory, které jsem na předchozích stránkách projevil berte jako názory člověka, který se již dva roky aktivně věnuje oblasti PKI a tedy elektronickým podpisům a který se aktivně podílí na vývoji jediné české certifikační autoritě, která má být určena pro komerční prodej.

Daniel Cvrček, ústav výpočetní techniky a informatiky, Vysoké učení technické v Brně