DIGITÁLNÍ PODPIS

Dagmar Brechlerová

Katedra informačních technologií PEF ČZU, Praha 6, Kamýcká ul., brechlerova@pef.czu.cz

Abstrakt

V referátu jsou vysvětleny základní pojmy týkající se digitálního podpisu. Je osvětlen postup tvorby podpisu a jsou objasněny některé základní právní náležitosti podpisu a současná situace v ČR.

Úvod

Široké používání informačních a komunikačních technologií vyvolalo v posledních desetiletích výrazné změny ve všech oblastech lidské činnosti. Elektronické obchodování umožňuje nyní i velmi malým podnikům přístup na globální trhy, informatizace společnosti vytváří předpoklady pro zefektivnění administrativy. Další možností je např. vzdělávání na dálku tzv. e- learning. Informatizace společnosti by mohla přispět také k většímu přístupu občanů k informacím a tedy k vzrůstu aktivity lidí ve všech sférách společenského života. Používání elektronicky pořízených, případně elektronicky podepsaných dokumentů umožňuje nepořizovat a poté neudržovat papírové kopie, data zadávat přímo do elektronických formulářů atd. V budoucnu bude možné přejít v některých situacích na čistě elektronické verze dokumentů. Často se dnes pro tuto změněnou situaci používá název Informační společnost.

Aby výše uvedené vize mohly být realizovány, je nutné splnit některé předpoklady. Základním předpokladem v této Informační společnosti je zabezpečení volného pohybu informací a zrovnoprávnění informací v elektronické podobě informacím v papírové podobě. Volný pohyb informací je nutno zajistit jednak legislativně (např. povinnost organizací poskytovat informace) a jednak technicky. Zrovnoprávnění elektronické a papírové podoby informací má aspekty právní a bezpečnostní. Řešením některých těchto problémů je elektronický podpis resp. jeho technická realizace pomocí tzv. digitálního podpisu.

Aby elektronický podpis mohl nahradit případně i více než nahradit ruční podpis, je nutné zajistit identifikaci podepisující osoby, neporušenost doručeného dokumentu tzv. integritu, nepopiratelnost – tj. autor podpisu nemůže poté popřít, že podepsal právě on a právní akceptovatelnost digitálního podpisu. Toto jsou základní požadavky kladené na digitální podpis. Někdy se k nim připojují ještě další požadavky např. možnost ujištění, že dokument existoval v daném čase (tzv. časové značky). Zde nutno podotknou, že digitální podpis sám o sobě neposkytuje utajení dokumentu. Chceme- li tedy dokument utajit, je nutno jej nejen podepsat, ale také zašifrovat veřejným klíčem příjemce, rozdíl bude vysvětlen v dalším textu.

Protože realizace digitálních podpisů je skutečně pro rozvoj informační společnosti zásadní, Evropská unie přijala směrnici 1999/93/EC, ze které poté vycházejí národní zákony o elektronickém podpisu. Pro členské země EU bylo zapotřebí včlenit tuto směrnici do 19.6.2001 do jejich legislativy. V ČR byl v minulých letech (v roce 2000) přijat příslušný

zákon [1], který celou problematiku v některých situacích upravuje, v jiných systémech není nutno se tímto zákonem řídit.

Podstata digitálního podpisu

Dále bude krátce zmíněna podstata digitálního podpisu. Pro podepisování se používá asymetrických algoritmů. Osoba A- Alice, která podepisuje, má dvojici klíčů. Dvojice klíčů jsou dvě čísla, která jsou svázána spolu tím, že vznikla při určité matematické operaci, nejedná se tedy o náhodnou dvojici. Jeden klíč se nazývá soukromý (tajný) a druhý veřejný. Soukromý klíč ("data pro podpis") je nutno uchovávat v tajnosti např. na čipové kartě, v trezoru apod. a používá se pro podepisování. Druhý tzv. veřejný klíč je nutno naopak vhodným způsobem zveřejnit, např. pomocí certifikační autority (viz dále) a ten se používá na ověřování podpisu. Veřejný klíč jsou tedy jedinečná data, svázaná jednoznačným způsobem s daty pro podpis a sloužící pro ověření elektronického podpisu. Nejznámějším a nejpoužívanějším asymetrickým algoritmem je RSA (1977, pojmenovaný podle autorů Rivest, Shamir a Adelmann), ale mohou se použít i asymetrické algoritmy založené na diskrétním logaritmu či eliptických křivkách.

Při podepsání dokumentu se postupuje tak, že se tento zdigitalizuje (je možno totiž podepsat text, zvukovou nahrávku, obraz atd.) Poté se z této digitalizované podoby pomocí hashovací funkce spočte tzv. hash hodnota (otisk zprávy aj. názvy). Hashovací funkce má tedy za úkol vytvořit otisk zprávy. Vstupem hashovací funkce je zpráva libovolně dlouhá, výstupem je otisk, který má určitou pevnou délku. Hashovací funkce jsou konstruovány tak, že pokud bychom ve zprávě změnili i jediný bit, dostaneme na výstupu úplně jiný otisk. Nejznámější hashovací funkce jsou MD5 (message digest, otisk 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk 160 bitů). Výstup hashovací funkce se zašifruje s pomocí soukromého klíče podepisující osoby. Číslo, které vznikne, se nazývá digitální podpis. Zde je nutno upozornit na významný rozdíl mezi klasickým a elektronickým, zde konkrétně digitálním podpisem. Klasický podpis je stále stejný a je tedy možno ověřovat jeho vzhled, porovnávat, je možno vytvořit podpisové vzory. Digitální podpis je ale pokaždé jiný, protože závisí na podepisovaném dokumentu a na soukromém klíči. (v našem zákonu použit termín na "datech pro vytváření elektronického podpisu"). Proto také není možné mít nějaké vzory podpisů, jako je tomu u klasických podpisů.

Pokud někdo – osoba B tedy Bob - ověřuje tento podpis, nejprve spočte také hash hodnotu dokumentu, který např. obdržel elektronickou poštou. Poté digitální podpis, který byl k tomuto dokumentu připojen, odšifruje pomocí veřejného klíče odesílatele a obě hash hodnoty porovná. Pokud jsou stejné, jsou splněny následující požadavky. Elektronicky podepsaný dokument se shoduje s původním dokumentem, tedy nebyla porušena integrita – to zaručuje stejná hodnota výsledku hashovací funkce, elektronický podpis vytvořil někdo, kdo měl přístup k dokumentu a k soukromému klíči podepisovatele. Z toho tedy vyplývá, že je skutečně nutno soukromý klíč velmi pečlivě chránit, tak aby nepadl do rukou někomu nepovolanému. Celý postup podepsání provádí program, ale ten opět musí splňovat určité právní požadavky.

Certifikáty a certifikační autority

Druhý významný problém je spojení veřejného klíče a jeho držitele, respektive důkaz, že veřejný klíč patří skutečně tomu, kdo to tvrdí. K tomu slouží často tzv. certifikáty. Certifikát je něco obdobného jako občanský průkaz. Je to elektronický dokument s přesně určenými

políčky, který vydá certifikační autorita. V tomto dokumentu je jméno držitele certifikátu (náš zákon umožňuje i pseudonym), veřejný klíč, doba platnosti a řada dalších údajů. Formát certifikátu je dán normou. V našem zákoně je specifikován následovně.

§ 12
Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat
- *a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,*
- *b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,*
- *c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,*
- *d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,*
- *e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,*
- *f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,*
- *g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,*
- *h) počátek a konec platnosti kvalifikovaného certifikátu,*
- *i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,*
- *j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.*

(2) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

Některé systémy používají certifikáty pro ověřování elektronického podpisu, jiné ale nikoliv. Certifikáty jako běžný způsob předávání dat pro ověřování elektronického podpisu (tedy veřejný klíč) používá například Microsoft Outlook či Outlook Express.

Data pro ověřování elektronického podpisu (veřejné klíče) lze také vystavit v internetové síti veřejných klíčů (tak to je u PGP) či na jakémkoliv jiném přístupném místě, kde se s nimi mohou zájemci o komunikaci seznámit. Pro ověření „pravosti“ dat pro vytváření elektronického podpisu se používá rovněž jejich podepisování jinou osobou (např. u PGP), předání jejich otisku (jednoznačné identifikace, angl. fingerprint) například na vizitce nebo zaslání e-mailem a následným ověřením jiným způsobem.

Nutno ale podotknout, že používání PGP pro elektronické podepisování není zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu, vydaným poskytovatelem certifikačních služeb ve smyslu našeho zákona o elektronickém podpisu.

Jak tedy získat certifikát toho s kým komunikuji? Většina běžně užívaných aplikací zasílá certifikát zároveň s elektronicky podepsanou zprávou, tedy obdržím zprávu, k ní připojený elektronický podpis této zprávy a k tomu připojený certifikát. Jinak musí podepisující osoba oznámit, kde je její certifikát dostupný (viz výše). Obvykle se jedná o server poskytovatele, který certifikát vydal, tedy certifikační autority nebo webovou stránku podepisující osoby.

Pokud chceme kromě podepsání zaručit také utajnění dokumentu, postupujeme tak, že dokument zašifrujeme veřejným klíčem příjemce, a je možno ho rozšifrovat pouze příjemcovým soukromým klíčem.

Zákon o elektronickém podpisu

Náš Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu, 227/2000 Sb, částka 68/2000 Sb.) byl přijat 29. června 2000 a rozeslán dne 26. července 2000, jeho účinnost je od 1. října 2000. Vyhlášky k tomuto zákonu, které upravují konkrétní technické realizace jako je druh šifrování, druh hash fukcí apod. byly přijaty v roce 2001.[2].

Některé základní pojmy z našeho zákona:

§ 2
Vymezení některých pojmů

Pro účely tohoto zákona se rozumí

a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě,

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky:
   1. je jednoznačně spojen s podepisující osobou,
   2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
   3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
   4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

c) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

d) podepisující osobou fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby,

e) poskytovatelem certifikačních služeb subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

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

g) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost,

h) kvalifikovaným certifikátem certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty,

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

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

k) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,

l) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,

m) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,

n) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,

o) nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,
p) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

Náš zákon tedy rozlišuje elektronický podpis EP § 2 a) a zaručený elektronický podpis ZEP. § 2 b)
U zaručeného elektronického podpisu jsou zákonem dány následující náležitosti.
1. fyzická osoba (podepisující osoba), která zprávu podepsala, nemůže poté popřít, že je původcem této zprávy,
2. je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána (zachování integrity zprávy),
3. je možné zjistit identitu podepsané osoby,
4. je zajištěna právní akceptovatelnost podpisu.

Náš zákon o elektronickém podpisu upravuje náležitosti pouze některých elektronických podpisů a některých druhů certifikátů, konkrétně tedy zaručeného elektronického podpisu a kvalifikovaného certifikátu a také podmínky pro některé poskytovatele certifikačních služeb, tedy pro ty, kteří vydávají kvalifikované certifikáty. Takoví poskytovatelé se mohou rozhodnout, že budou usilovat o získání akreditace, a to po splnění dalších povinností uložených zákonem a podmínek daných prováděcí vyhláškou.

Po udělení akreditace mohou své služby poskytovat v oblasti orgánů veřejné moci. Paragraf § 11 zákona o elektronickém podpisu totiž říká, že

§ 11
V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

Situace se ale nyní změnila tím, že v současné době (duben 2002) je zákon novelizován, Sněmovnou již prošla novelizace a Senátem prochází. Tato novelizace obsahuje následující text:

Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátu užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.".

Pokud novelizace projde, což je vysoce pravděpodobné, mohlo by v nejhorším případě i dojít k tomu, že pro kontakt s různými orgány v oblasti veřejné moci bychom potřebovali různé certifikáty, neboť každý tento orgán by si jednoznačnou identifikaci vysvětlil po svém. Je ale zbytečné předbíhat situaci. Pravdou je, že článek [5] vyvolal na dané téma širokou polemiku, kterou je možno sledovat na Internetu.

Pokud nejsme v oblasti orgánů veřejné moci, tj. např. při komunikaci v podniku, ve škole, s bankou atd., je na komunikujících subjektech, zda budou vyžadovat používání kvalifikovaných certifikátů ve smyslu zákona.

Současná situace

Častým případem, kde se uvádí možné užití digitálního podpisu je daňové přiznání fyzických osob. Zrovna zde ale není situace jednoduchá. Je zde totiž nutno přidávat další dokumenty jako potvrzení o zaplacení pojistného, příjmy od dalších zaměstnavatelů atd. Domnívám se, že podávání jiných dokumentů bude jednodušší. Problematice podávání daňových přiznání byl věnován velmi zajímavý článek na konferenci ISSS.[3]

V březnu roku 2002 byla v ČR udělena první akreditace a to za splnění následujících podmínek [4]
splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona o elektronickém podpisu;
splnění podmínek a požadavků stanovených vyhláškou č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu;
splnění požadavků na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku zveřejněné v souladu s § 2 odst. 7 vyhlášky č. 366/2001 Sb;
ověření kvalifikovaných certifikátů Úřadem pro ochranu osobních údajů podle § 10 odst. 7 zákona o elektronickém podpisu.

Tuto akreditaci získala První certifikační autorita, a.s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9. Zatím ale žádný z poskytovatelů certifikačních služeb nevydává kvalifikované certifikáty podle zákona č. 227/2000 o elektronickém podpisu. (situace březen 2002), ale to se jistě brzy změní.

Dá se říci, že nyní již nestojí kontaktu se "státní správou" nic v cestě. Situace ale není tak jednoduchá. Jednak bude nutno napsat aplikace, které budou použití digitálního podpisu podporovat, příslušné úřady se budou muset na tuto změněnou situaci připravit. K plnému odstranění papírových dokumentů je ještě dlouhá cesta a navíc je sporné, zda by to bylo vždy přínosem. V některých situacích to navíc naše zákony neumožňují.

Literatura:

1. http://www.uoou.cz/227_2000.php3
2. http://www.mvcr.cz/sbirka/2001/sb138-01.pdf
3. Faltýnek .M, Elektronický podpis v daňové správě, in http://www.isss.cz/2001/sbornik.asp
4. http://www.uoou.cz/ep_akreditace.php3
5. http://www.lupa.cz/clanek.php3?show=2200