MASARYKOVA UVIVERZITA V BRNĚ

PRÁVNICKÁ FAKULTA

ELEKTRONICKÝ PODPIS

PRAHA 2005 **FARID HANAFI**

PRÁVO A PODNIKÁNÍ

Úvod

Vzájemná komunikace je již od pradávna základem lidského společenství. Postupem času a s vývojem techniky jsme si osvojili její různé formy; od komunikace mluvené, písemné, přes telefonickou až po elektronickou, která se v současnosti stává neodmyslitelnou součástí života každého z nás.

Informace a dokumenty přenášené elektronicky mohou být různého stupně důležitosti, mohou mít charakter jak osobní, tak i pracovní nebo obchodní, z praktických důvodů je tedy nutné v nich jednoznačně určit autora. Nejčastěji se pod takové dokumenty podepisujeme textovým řetězcem, kterým zapíšeme svoje jméno. Další možností je vložení obrázku obsahujícího náš zdigitalizovaný – naskenovaný podpis. Takové podpisy nám ale nedávají žádnou právní záruku, vzhledem k tomu, že se dají velice jednoduše zneužít. Ještě donedávna se musely všechny dokumenty převtělit do klasické papírové podoby, která jako jediná umožnila provést poslední krok k uzavření smlouvy, a to sice její právoplatný podpis.

K zásadní změně uvedené situace u nás došlo přijetím zákona č. 227/2000 Sb., o elektronickém podpisu, na jehož základě může být právoplatný podpis proveditelný v rámci digitálního dokumentu bez potřebného vytištění na papír, a to připojením ověřitelného elektronického podpisu. Ten se dá využít všude tam, kde se dnes užívá běžný psaný podpis. Výhodou je nesrovnatelně rychlejší, přesnější a jednodušší ověřitelnost, ale také možnost podepsat se i pod to, co se dá jinak ověřit jen velmi těžko, např. obsah diskety, fotografie, přístupy do databáze atd.

Co je to elektronický podpis?

Elektronický podpis nelze popsat jednoduchou definicí, protože tento pojem v sobě zahrnuje technické, kryptologické, normotvorné a právní hlediska. Zákon o elektronickém podpisu (Zákon č. 227/2000 Sb.) definuje elektronický podpis jako „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“. Tato definice však také znamená, že elektronickým podpisem je i to, když se podepíšeme nakonec e-mailu nebo textového dokumentu. Takovýto podpis však nemá příliš velkou hodnotu.

Aby byl elektronický podpis akceptovatelný jako podpis vlastnoruční, musí hlavně zajišťovat:

-neporušenost dokumentů - je nutné zajistit, aby dokumenty, soubory, e-maily nemohly být po podepsání měněny

-identifikaci podepisující osoby - každý elektronický podpis je jedinečný, je úzce spjat s osobou, které patří a v případě nutnosti osobu identifikuje

-nepopiratelnost podpisu - je nutné zajistit, aby osoba, která se podepsala, nemohla později podpis popřít

-nepopiratelnost podpisu - je nutné zajistit, aby osoba, která se podepsala, nemohla později podpis popřít

-existence podpisu v daném čase - bude možné prokázat, že dokument, e-mail byl podepsán v konkrétním časovém okamžiku.

Všechny uvedené vlastnosti zajišťuje „zaručený elektronický podpis“ definovaný Zákonem o elektronickém podpisu. O zaručeném elektronickém podpisu používající kryptografické metody hovoříme jako o **digitálním podpisu**.

Realizace elektronického podpisu

Elektronický podpis v současné době využívá vlastností kryptografických algoritmů s veřejným klíčem. Tyto algoritmy charakterizuje základní princip, který spočívá v konstrukci *dvojice jednoznačně matematicky svázaných různých klíčů*. Jedná se o **veřejný klíč**, který se využívá k zašifrování zpráv a je publikován, naproti tomu **privátní klíč**, určený k dešifrování přijaté zprávy musí být pečlivě chráněn a zůstat před ostatními utajen. Zašifrujeme-li danou zprávu veřejným klíčem příjemce, pak pouze on s pomocí svého privátního klíče může tuto zprávu dešifrovat a přečíst. Důležité je, že dvojice klíčů daného algoritmu je navržena tak, aby nebylo možné ze známého veřejného klíče získat, vypočítat či odvodit klíč privátní.

Uživatel, který chce ke své zprávě připojit elektronický podpis, použije k tomu svého privátního klíče. Každý, kdo zná jeho veřejný klíč může pomocí tohoto klíče ověřit připojený podpis a ví, že zprávu mohl odeslat *pouze on*, neboť vlastní příslušný privátní klíč.

Bezpečnost elektronického podpisu

Z realizace elektronického podpisu pak plynou i jeho bezpečnostní záruky. Ty se váží zejména na ochranu privátního a veřejného klíče kryptoalgoritmu. Bezpečnost při používání elektronického podpisu je postavena na tom, že:

- Nemohlo dojít k narušení tajnosti privátního klíče.
- Nebyl prolomen použitý kryptoalgoritmus ani narušena kryptologická bezpečnost hash funkce.
- Nedošlo k porušení autentičnosti veřejného klíče a tím nedodržení záruky, že deklarovaný veřejný klíč přísluší osobě, která zprávu podepisovala.

Aby byla splněna třetí bezpečnostní podmínka, je v případě používání kryptoalgoritmů typu *RSA* nebo *DSA* v prostředí s velkým počtem uživatelů využíván systém certifikátů poskytovaných nezávislou třetí stranou - *certifikační autoritou* (poskytovatelem certifikačních služeb).

Ještě před získáním certifikátu s privátním klíčem je nutné rozhodnout se, kam jej budeme chtít uložit. Certifikát si totiž nesmíme představovat jako kus krásně potištěného papíru, ale jako datové soubory, tedy něco nehmatatelného. Jedná se o soubory veřejného a osobního klíče. Jak z jejich názvu vyplývá, veřejný klíč slouží ke zveřejnění, a taky k ověření autenticity e-podpisu, osobní klíč musí být naopak velmi pečlivě utajen, protože právě s jeho pomocí vytváří počítač unikátní e-podpis ke každé zprávě. A jsme u jádra problému. Soubory certifikátu jsou sice malé a mohou být uloženy na harddisku počítače. Dokonce jsou chráněny PINem. Pokud je však nemáte zazálohovány na nějakém paměťovém médiu (např. disketa či CD-ROM), může se stát, že bude nutno přeinstalovat operační systém počítače a v tom okamžiku o certifikát přijdete. Pokud si zálohu pořídíte, je to potenciální nebezpečí jak může dojít ke kompromitaci osobního klíče. Druhou možností je použít nějaké bezpečné úložiště. Tím může být čipová karta nebo USB token. Tyto prostředky se připojují k počítači a soubory certifikátu z nich nelze žádným způsobem dostat ven. Samozřejmě pojmou i víc certifikátů a lze je použít i k dalšímu zabezpečení počítače. Při použití čipové karty musí být k počítači připojena její čtečka a čipovou kartu lze použít všude tam, kde taková čtečka je. USB token čtečku nepotřebuje, na počítači však musí být nainstalovány jeho ovladače, což je ovšem snadná záležitost. Pro firmy bývá obvykle lepší čipová karta, pro jednotlivce, který nepotřebuje certifikáty používat v různých organizacích, bývá lepší USB token.

Certifikační autorita

V prvé řadě musí existovat někdo důvěryhodný, kdo ověří vaši totožnost a vydá certifikát, na základě kterého váš počítač generuje pro odesílané zprávy konkrétní e-podpisy. Tím někým důvěryhodným jsou certifikační autority. Na vás je vybrat si některou CA a u ní si zažádat o vystavení certifikátu. Obvykle lze tuto žádost podat prostřednictvím internetu. Výběr CA záleží na tom, k jakým účelům certifikát potřebujete. Jedná-li se o komunikaci se státní správou, musíte mít certifikát zaručený a

ten vydávají pouze některé CA. Pokud tedy pomineme oblast komunikace se státní správou, nepotřebujeme certifikát zaručený a zde je již výběr CA podstatně širší.

Certifikační autorita plní dvě základní funkce:

- *certifikační* – zaručující, že deklarovaný veřejný klíč přísluší dané osobě,
- *validační* – potvrzující platnost certifikátu.

V *případě certifikace* se jedná o vydávání certifikátů uživatelům, kdy certifikát je dokument, který stvrzuje, že veřejný klíč (uvedený na certifikátu) patří jednoznačně dané osobě. Certifikát zároveň obsahuje další informace týkající se uživatele, doby platnosti klíče, informace o používání klíče a informace o certifikační autoritě. Certifikát je podepsán elektronickým podpisem certifikační autority. A jeho struktura vesměs odpovídá doporučení mezinárodní organizace *ITU - X.509.v3* .

V *případě komunikace* mezi dvěma uživateli si uživatelé nejdříve ověří podpis svého partnera pomocí jeho veřejného klíče a posléze si ověří autentičnost veřejného klíče partnera ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority. V daném případě se požadavek na důvěryhodnost vztahuje pouze k certifikační autoritě.

V *případě validace* se uživatel dotazuje u certifikační autority na platnost certifikátu svého partnera. Systém dotazů může být řešen on-line nebo i využitím seznamu neplatných certifikátů (*CRL*), tj. seznamu certifikátů, jejichž platnost byla ukončena před stanovenou dobou platnosti.

Elektronický podpis a EU

Elektronické podpisy nemají z legislativního pohledu ve světě příliš dlouhou tradici. Státy Evropské unie pochopily nezbytnost jednotného přístupu k elektronickému podpisu (jde zejména o návaznost společného trhu a elektronického obchodu) a vydala v roce 1999 Směrnici o zásadách pro elektronické podpisy, kde bylo stanoveno pouze určité nezbytné minimum s tím, že budou následovat další kroky upravující v rámci stávajícího právního rámce další otázky, např. odpovědnost za škodu, obchodování na dálku, atd. Tato Směrnice je tedy velmi obecná a obsahuje řadu kompromisů.

Vychází z řady základních principů:

- technologická neutralita – Směrnice tedy výslovně nehovoří o žádné konkrétní technologii, což otevírá prostor pro řadu dalších metod a řadu dalších technologických principů
- neexistence jakéhokoliv přímého či nepřímého omezení týkající se počtu poskytovatelů certifikačních služeb

- rozpoznání zákonné platnosti elektronických podpisů tak, aby nemohla být popřena jejich platnost na základě toho, že jsou v elektronické podobě, a byla zaručena ekvivalence s ručně napsaným podpisem. S tím souvisí i požadavek uznávání elektronických podpisů jako důkazních prostředků v soudním řízení, který výslovně zakazuje členským zemím omezovat použitelnost e-podpisu jako důkazních materiálů na základě toho, že mají elektronickou podobu.
- pro autorizaci není poskytovatelům certifikačních služeb definováno šablonové schéma pro autorizaci, takže do budoucna existuje principiální možnost technologických inovací.

Závěr

Elektronický podpis je řešením, které nepochybně zefektivňuje řadu běžných činností, čímž se snad podaří odstranit některé problémy související se skutečností, že je stále větší poptávka po využívání elektronických médií i pro nejrůznější úkony, pro které je v dnešní době stále ještě vyžadována „papírová forma“ včetně vlastnoručního podpisu. Často uváděným příkladem může byt právě předkládání daňových přiznání v elektronické formě. Obecně však jde o podstatně širší škálu právních úkonů začínající u spolehlivé komunikace a končící u uzavírání smluvních vztahů elektronickou cestou. Praktické používání elektronických podpisů přináší výrazné zefektivnění, zjednodušení a také zlevnění řady úkonů, a to doslova pro každého, státní správou počínaje, přes soukromý sektor až po jednotlivé fyzické osoby. Prosazení elektronických podpisů do praxe je tedy v zájmu všech profesních sdružení včetně těch právnických.

Použitá literatura

D. Bosáková, A. Kučerová, J. Peca, P. Vondruška: Elektronický podpis. Nakladatelství ANAG, Praha 2002

http://www.e-podpis.bod.cz

http://www.fzu.cz