MASARYKOVA UNIVERZITA V BRNĚ
PRÁVNICKÁ FAKULTA

Elektronický podpis – význam pro komunikaci elektronickými prostředky

(seminární práce)

Lýdia Regéciová, UČO: 108551

Brno 2005

Úvod

Snad každý z nás se v životě setkal s výzvou: „přečtěte si to a pokud s tím souhlasíte, podepište to“. Běžný podpis nám v každodenním životě poskytuje jakési záruky. Prokazuje skutečnost, že podepsaná osoba byla přítomná na stanoveném místě; poskytuje důkaz, že se podepsaná osoba cítí s obsahem dokumentu vázáná, či již jako autor textu dokumentu nebo v případě, že dokument sestavila jiná osoba, potvrzujeme svým podpisem ztotožnění se s obsahem.

U papírových dokumentů se identifikace podepisující se osoby provádí obvykle uvedením jména a příjmení a autentizace se provádí podpisem, který může příjemce srovnat s jemu známým podpisovým vzorem (např. v případě banky), nebo lze v případě sporu pravost podpisu ověřit posudkem soudního znalce.

Ale co v případě využití informačních a telekomunikačních systémů? Jak zajistit, aby šířené informace byly dostupné jenom oprávněným osobám? Jak zajistit správnost, kompletnost, neodmítnutelnost odpovědnosti, nepopíratelnost určitých operací? Jak splnit požadavek důkazného prostředku pro právní úkon? Významný nástroj zde představuje elektronický podpis.

1. Elektronický podpis

Elektronický podpis je obvykle chápán jako číslo, které vytváří podepisující osoba pomocí svých dat pro vytvoření elektronického podpisu a pomocí zprávy, kterou podepisuje. V podstatě se jedná o implementaci určité matematické funkce prostřednictvím specializovaného programu, jejímž připojením k určitému dokumentu dochází k ověření jeho pravosti. Odborníci tady mluví o kryptografické metodě tzv. hashování, kdy obsah dokumentu (velké číslo) je převedeno na kratší číslo. Vzhledem k obsahu dokumentu je jednoznačné a má pevnou délku. Místo podpisu máme k dispozici druhé číslo – tajné podpisové, tzv. privátní klíč. Matematickým spojením těchto dvou čísel vzniká číslo nové, tj. digitální podpis.

2. Typy elektronických podpisů

Celý systém elektronického podepisování dokumentů u nás upravuje zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Tento zákon vymezuje v § 2 kromě základních pojmů i požadavky, na základě kterých se dá mluvit o několika typech elektronického podpisů:

- elektronický podpis (§ 2 písm. a) – jsou to údaje v elektronické podobě, které jsou k datové zprávě připojené nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě; nejsou kladeny žádné speciální požadavky na použitý podpisový systém nebo na prostředek pro vytváření, případně ověřování elektronického podpisu; nepožaduje se časové razítko, není definován žádný konkrétní formát nebo standard, není použit certifikát; tento typ podpisu nemá pro příjemce příliš velkou vypovídací hodnotu a důvěra v něj je minimální, slouží spíše pro informaci příjemce; příkladem je „podpis“ vložený pod klasický e-mail
- zaručený elektronický podpis (§ 2 písm. b) – zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:
  - je jednoznačně spojen s podepisující osobou
  - umožňuje identifikaci podepisující se osoby ve vztahu k datové zprávě
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou

- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat

- zaručený elektronický podpis založený na kvalifikovaném certifikátu – k použití tohoto typu podpisu se vážou pojmy certifikát, kvalifikovaný certifikát a pojem poskytovatel certifikačních služeb (viz. klíčová slova)
- kvalifikovaný podpis určený pro archivaci dat – je představen ve standardu ETSI, ve kterém jsou zformulovány minimální požadavky v oblasti bezpečnosti a kvality zabezpečení důvěryhodného poskytování služeb určených k vydávání časových razítek; využití je zřejmé: dlouhodobá archivace elektronicky podepsaných dokumentů v elektronické podobě

Kromě uvedeného zákona o elektronickém podpisu doporučuji k prostudování i další právní normy a dokumenty týkající se této problematiky, např. směrnice ES o elektronickém podpisu; dokumenty OSN pro mezinárodní právo (UNCITRAL) a další.

3. Využití elektronického podpisu

Pokud se rozhodnu elektronicky podepisovat své datové zprávy, mohu již v současnosti tento způsob svojí autorizace uplatnit v elektronickém obchodování, při komunikaci se svojí bankou a navíc, právě díky legislativním a technickým změnám i při jednání se správními úřady. Aby byl můj podpis důvěryhodný pro příjemce zprávy začnu používat elektronický podpis založený na certifikátu. Certifikát získám od poskytovatele certifikačních služeb. Nabídku těchto certifikačních autorit mohu vyhledat na Internetu. Odlišují se rozsahem služeb, které nabízí a samozřejmě cenou. Obvykle je žádost o vydání certifikátu přístupná na webových stránkách poskytovatelů. Stačí ji vyplnit a vytvořit dvojice dat pro vytváření elektronického podpisu (soukromý klíč) a dat pro ověřování elektronického podpisu (veřejný klíč). Data pro vytváření podpisu tvoří s daty pro ověřování podpisu pevnou dvojici. Nelze nahradit, vyměnit nebo podvrhnout žádnou jejich část, aniž by tím nabyla narušena jejich vazba. Poskytovatel vydá certifikát, v němž jsou uvedena data pro ověřování podpisu, údaje o majiteli, údaje o poskytovateli, údaj o počátku a konci platnosti certifikátu nebo údaje o omezení použití certifikátu. Lze si nechat vystavit několik certifikátů, každý pro jiný účel.

Poskytovatel opatří vydávaný certifikát svým elektronickým podpisem. Certifikát je vydán ve formě datové zprávy. Příjemce ho dostává zároveň se zprávou nebo mu sdělíme, kde je certifikát dostupný – na klíčovém serveru, na vlastních webových stránkách apod. Data pro vytvoření podpisu máme obvykle uložena na pevném disku počítače, který užíváme nebo na disketě, čipové kartě či jiném přenosném nosiči.
Když vytvořím zprávu, kterou chci odeslat, zadám příkaz (např. kliknu na příslušnou ikonu), aby byla zpráva elektronicky podepsaná . To co se následně děje na svém monitoru nevidím a ani se toho procesu již nijak neúčastním. K mojí zprávě je přiložen elektronický podpis. Příjemce zprávy taky nezasahuje do procesu ověřování – většina dnešních aplikací sama ohlásí, že úspěšně ověřila podpis. Příjemce si ověřuje jenom platnost certifikátu – poskytovatelé vydávají seznam zneplatněných certifikátů na webu, tzv. CRL (certificate revocation list).
Elektronicky lze podepisovat nejen textové zprávy, ale vše, co existuje v elektronické podobě, např. obrázek, program, databázový soubor, makra apod.

Klíčová slova

certifikační autorita – poskytovatel certifikačních služeb, který je důvěryhodný pro uživatele, tj. pro podepisující osoby, kterým vydává certifikáty, tak i pro osoby, které se spoléhají na podpisy, s nimiž jsou certifikáty spojeny
certifikát – datová zpráva vydána poskytovatelem certifikačních služeb; slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu
kvalifikovaný certifikát – certifikát, jehož obsah stanovuje zákon o elektronickém podpisu v § 12

Závěr

Domnívám se, že v současnosti není možnost zneužití elektronického podpisu větší, než u podpisu ručního. Docent Smejkal a řada dalších odborníku na informační technologie dokonce uvádí, že možnost ověření pravosti elektronického podpisu je daleko vyšší. Osobně jsem se již setkala s pozměněnými dokumenty, s padělanými veřejnými listinami, se zneužitím PINu, ale s pochybením v souvislosti s elektronickou identifikaci a autorizaci zatím ne. Proto má elektronický podpis mojí důvěru a jsem přesvědčená, že jeho budoucnost je v širokém využití při podnikání, obchodování i nezbytné komunikaci s úřady. Odpadne nám nutnost osobních jednání, telefonických ověřování či jiných úkonů, které doposud používáme při své práci. A to nejenom při jednání s partnery vzdálenými pár desítek, ale i tisíce kilometrů, tudíž i v mezinárodním obchodě.

Literatura

1) Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 2.aktualizované a rozšířené vydání. Praha: C. H. Beck, 2004. 770 s.

2) kol.: Elektronický podpis. První vydání. Olomouc: ANAG, 2002. 144 s.

3) Přibyl, T. a kol.: Svět elektronického podpisu. PC world: AEC – data security company, 2000.58 s.