PROBLEMATIKA DIGITÁLNÍHO PODPISU
PROBLEMS OF DIGITAL SIGNATURE

Eva Jablonská, RNDr.,CSc., KIT PEF ČZU Praha, jablonska@pef.czu.cz

Anotace:

Elektronický obchod je jednou z možností, jak zvýšit konkurenceschopnost podniku. V této souvislosti je nezbytné zajistit nejen bezpečnost dat, ale také omezit možnost vysílat falešné zprávy, což lze zabezpečit např. digitálním podpisem. Článek se zabývá některými aspekty této problematiky.

Summary:

Some aspects of a digital signature are discussed.

Klíčová slova:
digitální podpis, elektronický obchod
Keys words:
digital signature, electronic business

Přenos informací prostřednictvím počítačových sítí v oblasti obchodu a administrativy prudce narůstá. Elektronický obchod pro koncové zákazníky přináší nepopiratelnou konkurenční výhodu podniku mj. snížením nákladů. Pro následující roky se předpokládá značné navýšení objemu obchodů přes Internet. Pro zvýšení zájmu zákazníků je však třeba nejen speciální služba pro doručování zboží v dohodnutém čase (místo zasílání zásilek poštou na dobírku), ale především ochrana důvěrných informací přenášených v otevřené počítačové síti typu Internet a možnost ověření identity partnera. Digitální dokumenty, tj. dokumenty vytvořené v elektronické formě kódované digitálními kódy, je tedy třeba při přenosu v síti nejen chránit před neoprávněným přístupem, ale i kontrolovat, zda nebyly padělány, poškozeny nebo pozměněny.

Pro utajení obsahu digitálního dokumentu se používá šifrování. Zjištění skutečného zdroje informací, které je často neméně důležité, lze zajistit digitálním podpisem. Digitální podpis zajišťuje ještě další funkce, které lze shrnout takto (viz [1]):

- **autentizace** původce digitálního dokumentu, tzn. jednak příjemce bezpečně ví, kdo je autorem nebo odesilatelem digitálního dokumentu a má jistotu, že digitální dokument nebyl padělán nebo podvržen, jednak si nemůže někdo vyrobit digitální dokument a předstírat, že tento dokument obdržel od někoho jiného
- **integrita** (celistvost) digitálního dokumentu, tzn. příjemce digitálního dokumentu má jistotu, že digitální dokument nebyl modifikován

- **nepopiratelnost** (neodmítnutelnost odpovědnosti), tzn. odesilatel nebo autor nebude moci popřít, že daný dokument s daným obsahem vytvořil nebo odeslal

První dvě funkce lze zajistit technickými prostředky, k zabezpečení nepopiratelnosti je třeba legislativní podpory v zákoně o digitálním podpisu, který by měl zajistit rovnoprávné postavení vlastnoručního a digitálního podpisu, papírových a digitálních dokumentů.

Jeden z věcných záměrů tohoto zákona zpracoval Úřad pro státní informační systém (ÚSIS) [2], další návrh předkládá Sdružení pro informační společnost (SPIS) [7]. V návrzích jsou vzaty v úvahu jednak dokumenty na evropské i mezinárodní úrovni, které vymezují rámec pro přijetí národních zákonů o elektronickém obchodu a digitálním podpisu (Sdělení Evropské komise COM (97)503 z října 1997 "Evropský rámec pro digitální podpisy a šifrování" a Návrh směrnice Evropského parlamentu a Rady o společném rámci pro elektronické podpisy COM (1998)297), jednak zkušenosti z praktického používání a současný stav legislativy o digitálním podpisu ve světě.

Technické řešení digitálního podpisu

Samotný digitální dokument může být, ale nemusí být během přenosu zašifrován. Pokud se šifruje, je pro šifrování většinou použita vhodná symetrická šifra, která umožňuje rychlé zašifrování a odšifrování textu (např. DES - Data Encryption Standard nebo IDEA). Při symetrickém šifrování se používá pro zašifrování a odšifrování stejný číselný kód zvaný klíč. Přenos tohoto klíče mezi odesílatelem a příjemcem před zahájením přenosu je možno zabezpečit zašifrováním asymetrickou šifrou.

Asymetrický šifrovací systém (kryptografie s veřejným klíčem) je založen na principu jednocestných funkcí. U těchto funkcí lze snadno pro každé x vypočítat y = f(x), ale zpětný výpočet, kdy z hodnoty f(x) se má zjistit x, již jednoduchý není. Příkladem jednocestné funkce, která je základem známé asymetrické šifry RSA, je funkce, která přiřadí pro dvě velká (např. stomístná) prvočísla jako funkční hodnotu jejich součin. Zpětné rozložení součinu na činitele je pro takto velká čísla v reálném čase prakticky beznadějné.

Při asymetrickém šifrování si každý uživatel vygeneruje současně dva odlišné navzájem matematicky související klíče určité délky. Jeden klíč (soukromý, tajný) drží v tajnosti, druhý klíč (ověřovací, veřejný) zveřejňuje. Odvození soukromého klíče na základě znalosti veřejného klíče je přitom prakticky nemožné. Pokud chce odesílatel poslat zašifrovanou zprávu příjemci, zašifruje ji veřejnou šifrou příjemce a pouze příjemce může zprávu rozšifrovat svým soukromým klíčem.

Tento proces lze také otočit, odesílatel může dokument zašifrovat svým soukromým klíčem a příjemce ji může dešifrovat veřejným klíčem odesilatele. Tento způsob se používá pro digitální podpis. Pouze jedna osoba může digitální dokument podepsat, různí příjemci si mohou tento digitální podpis ověřit pomocí veřejného klíče odesílatele.

Použití asymetrického šifrování na celou zprávu je pro rozsáhlé zprávy pomalé. Lepší postup je použití bezpečné hašovací funkce, která vytvoří z celého dokumentu krátký výstup, zvaný Hash, který jednoznačně vypovídá o obsahu digitálního dokumentu.

Silná hašovací funkce musí být nekolizní, tzn. nesmí dávat pro dva různé dokumenty stejnou hodnotu Hash (tzn. při změně jediného bitu dokumentu má Hash jinou hodnotu než původně) a z dané hodnoty Hash nesmí být možné odvodit původní dokument. Místo celé zprávy se potom zašifruje soukromým klíčem uživatele pouze Hash a připojí se za digitální dokument jako digitální podpis. Na straně příjemce vyhledá počítač příslušný veřejný klíč odesilatele a dešifruje podpis. Tento dešifrovaný Hash se porovná s hodnotou Hash, který si příjemce vypočítá z přeneseného digitální dokumentu. Při shodnosti obou Hash má příjemce jistotu, že dokument nebyl modifikován nebo padělán.

Certifikační autorita

Příjemce nemá ale jistotu o identitě autora digitálního dokumentu (vlastníka příslušného veřejného klíče), nemá totiž jistotu, že veřejný klíč, kterým byl digitální podpis ověřen, opravdu patří uvedenému autorovi. Toto potvrzení identity vlastníka veřejného klíče může získat od třetí nezávislé důvěryhodné strany, která se v této souvislosti nazývá certifikační autorita (CA), která vydává certifikáty. Certifikát je digitální dokument podepsaný digitálně certifikační autoritou, který potvrzuje shodu veřejného klíče s dalšími informacemi, jako je např. jméno majitele veřejného klíče. Certifikát by měl mít omezenou délku platnosti – např. maximálně tři roky.

V rozsáhlých sítích certifikace klíčů příliš zatěžuje jednu certifikační autoritu a není vhodné soustřeďovat příslušné informace pouze do jednoho místa. V praxi se tedy zřizují víceúrovňové certifikační autority, kdy nejvyšší CA může udělovat licence pro podřízené certifikační autority.

Digitální podpis lze použít nejen při elektronickém obchodování pomocí Internetu, ale také ve státní správě při vzájemné komunikaci jednotlivých orgánů státní správy, styku občanů s orgány státní správy (daňová přiznání) i při provozování elektronického obchodu státními institucemi, při provádění právních úkonů v datových sítích nebo pro identifikaci osob v informačních systémech.

Literatura :

[1] Hanáček,P.: Proč potřebujeme zákon o digitálním podpisu,Seminář AFOI 1999, s.67-69

[2] http://www.usiscr.cz/cz/archiv/dokumenty/diskuse/dig_podpis.html

[3] Dobda,L.: Ochrana dat v informačních systémech, Grada, 1998

[4] Dohnal,J., Pour,J.: Řízení podniku a řízení IS/IT v informační společnosti, VŠE Praha, 1999, ISBN 80-7079-023-7

[5] Cheswick,W.R.,Bellovin,S.M.:Firewally a bezpečnost Internetu, Science 1998

[6] Vaníček,J.,Vaníček P.:Kdy bude zpráva z počítače právoplatným dokladem, Hospodářství 6/99 s.31-33, 7/99 s.25-29

[7] http://www.spis.cz