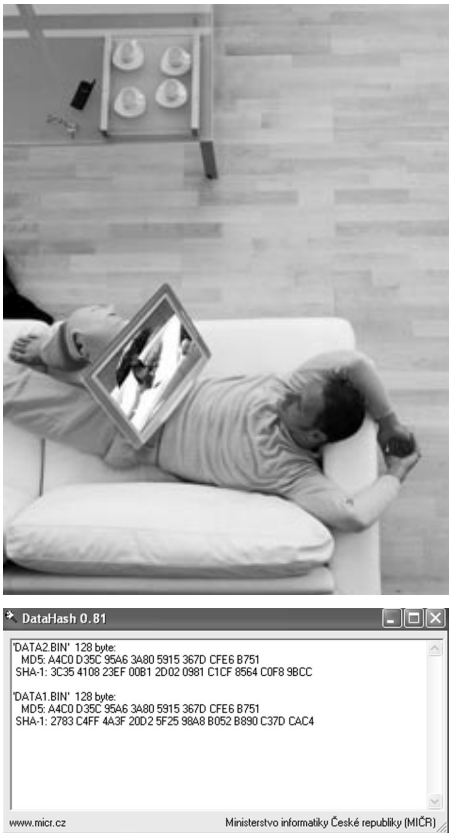
Kryptologie pro praxi – platforma elektronického podpisu

Fenomén elektronického podpisu je zaručenou rozbuškou vášnivých debat na téma příliš pomalého či naopak příliš zbrklého nástupu informatiky do běžného života občanů naší republiky. Jedněm se zdá, že zákon o elektronickém podpisu [5] a navazující vyhláška [4] spolu s další legislativou (viz portál [3]) jsou příliš vágní a tudíž nepoužitelné, jiní zase považují tyto prameny za dostačující a viní příslušné orgány a společnosti z laxního přístupu k jejich využívání. Další by zase nejraději, kdyby se radostné brouzdání internetem a oddané využívání každé nové prkotiny stalo nejdůležitější lidskou (nejlépe však i zvířecí) potřebou, atd... Z pohledu našeho seriálu jsou ovšem tyto aspekty druhořadé. Naším cílem je stručně uvést věcnou stránku elektronického podpisu jakožto můstku mezi kryptologickou konstrukcí podpisových schémat (viz ST 8/2003 a další, [6]) a právním rámcem úkonů jako je uzavření smlouvy, podání daňového přiznání, atp.

Stěžejním pramenem je zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, který byl od svého vydání již celkem třikrát novelizován, naposledy zákonem č. 440/2004 Sb. Elektronický podpis je zde definován (§2 písm. a)) jako *údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*. Odtud lze například odvodit, že i text „Prezident České republiky" může být v kontextu určitých zpráv chápán jako elektronický podpis konkrétní osoby. Jasně tak vidíme nutnost rozlišovat mezi pojmy elektronický a digitální podpis. Druhý z nich totiž už ve své definici zahrnuje základní bezpečnostní požadavky (nepadělatelnost, integrita, atd.). Tento aspekt v případě zákona přichází až s definicí zaručeného elektronického podpisu (§2 písm. b)), který již zavádí požadavky zhruba odpovídající kryptologickým postulátům digitálního podpisu [2]. Je vhodné předeslat, že zákon [5] v rámci možností abstrahuje od konkrétní technologie použité pro tvorbu (zaručených) elektronických podpisů. Nad jeho rámec se ovšem předpokládá, že nejvhodnějším kandidátem je v současnosti právě platforma digitálního podpisu, s čímž pak už implicitně pracuje navazující vyhláška [4]. Ze stejného předpokladu pro jednoduchost vyjdeme i zde.

Z praktického hlediska lze hlavní náplň zákona [5] spatřovat ve dvou bodech: Zaprvé v ukotvení právní možnosti podepisovat elektronické dokumenty elektronicky a zadruhé v zajištění určitého stupně důvěryhodnosti tohoto nástroje. Prvního cíle je kromě dílčích úprav ostatních zákonů dosaženo v §3 odst. 1, kde se mj. praví, že *datová zpráva je podepsána, pokud je opatřena elektronickým podpisem*. Všimněme si, že ani zde zákon apriori netrvá na zvláštních bezpečnostních aspektech. Druhou úlohu zákon a navazující vyhláška [4] řeší důrazem na



Obr. 1 Memento kolizí hašovací funkce MD5 (ST 12/2004) v jednom z nástrojů elektronického podpisu [3]. Díky kombinaci s funkcí SHA-1 je riziko eliminováno

kvalitu služeb certifikačních autorit a bezpečné nástroje elektronického podpisu. Až na výjimky (např. §11) však zákon nepředepisuje, jaký stupeň důvěryhodnosti podpisu (prostý elektronický nebo zaručený), certifikátu a nástroje (viz dále) má být kdy použit. Předpokládá se, že příslušné subjekty, spoléhající se na elektronicky podepsané zprávy, si ve svých obchodních podmínkách zvolí kvalitativní požadavky samy. S ohledem na aktuální stav technologie je toto asi rozumný přístup. Potenciálním rizikem tu ovšem je nutnost jisté erudice na straně uživatelů, kteří si musí být také schopni stanovit základní kriteria pro zapojení se do nějaké elektronické služby. Například by asi nebylo moudré souhlasit s tím, že své objednávky u příslušného obchodníka budou autorizovat elektronickým podpisem typu „Máňa ze Lhoty, ml.".

Certifikáty středem pozornosti

Důvěryhodnost certifikátů jakožto datových zpráv spojujících konkrétní podepisující osobu s daty pro ověřování elektronických podpisů (de facto veřejným klíčem) zásadním způsobem ovlivňuje i důvěryhodnost podpisů na nich založených. Zákon i vyhláška se proto markantně věnují právě definici takzvaných kvalifikovaných certifikátů (§12), kvalifikovaných poskytovatelů certifikačních služeb (§6) a jejich dozoru a případné akreditaci (§9). Cílem je zde definovat základní náležitosti takových certifikátů, politiku elementárních služeb s nimi spojených a v neposlední řadě též kontrolní mechanizmy umožňující pověřeným orgánům (zejména Ministerstvu informatiky) prověřovat, že vše opravdu funguje tak, jak má. Seznam poskytovatelů kvalifikovaných certifikačních služeb (kam náleží i kvalifikovaná časová razítka, viz dále) včetně těch, jimž byla udělena akreditace, lze nalézt na webových stránkách ministerstva [3].

Bezpečné nástroje

Kromě procesů vydávání a správy certifikátů (de facto certifikátů veřejných klíčů) ještě velmi záleží na ošetření rizika zneužití takzvaných dat pro vytváření elektronických podpisů (de facto privátního klíče) či zmatení prostředku pro ověřování podpisů. Za tímto účelem zákon a zejména vyhláška definují kriteria, podle kterých může být konkrétnímu nástroji udělen přívlastek „bezpečný". Toto udělování provádí příslušný odbor Ministerstva informatiky a aktuální seznam bezpečných nástrojů je vystaven na jeho stránkách [3]. Ideálním stavem by samozřejmě bylo, aby každý prvek systému byl označen jako bezpečný. S ohledem na vyspělost běžných aplikací (většina z nich dosud chápe bezpečnost toliko jako zajímavý marketingový slogan) a striktní požadavky vyhlášky to však zatím nejspíš nebude vždy možné. Architekti by se nicméně měli postupně snažit osazovat bezpečné nástroje (může se jednat třeba „jen" o dílčí kryptografický modul) všude, kde to bude s ohledem na rozpočet jen trochu možné.

Elektronické značky a časová razítka

Pojem elektronická značka (§2 písm. c)) byl zaveden při poslední novelizaci zákona k odlišení podpisu „lidského" od podpisu „stro-

jového“. Je zřejmé, že oba druhy podpisu bude nejspíš vyrábět nějaký elektronický nástroj, avšak u prvního z nich se implicitně předpokládá mnohem těsnější vazba ke konkrétní fyzické osobě, která by se například měla s obsahem každé podepisované zprávy před jejím podpisem seznámit (§3 odst. 1). Naproti tomu označující osoba v podstatě pouze výhradně kontroluje určité zařízení, které je schopno podle definované politiky označovat datové zprávy automatizovaně bez přímého ověření obsahu zprávy označující osobou (§3a odst. 2). Při postulování vlastností elektronické značky (§2 písm. c)) je už rovnou myšleno i na bezpečnostní aspekty, a to v rozsahu srovnatelném s nároky na zaručený elektronický podpis. Pod aplikací používající elektronické značky si můžeme představit například právě certifikační autoritu vydávající kvalifikované certifikáty. Jiným příkladem je autorita vydávající kvalifikovaná časová razítka. Tento pojem byl rovněž zaveden novelizací v roce 2004 a má umožnit důvěryhodným způsobem prokázat, že uvedená data v elektronické podobě existovala před daným časovým okamžikem (§2 písm. r)).

Závěr

Karikaturista by možná řekl, že platforma elektronického podpisu nepřinesla do elektronického světa nic nového, a z jistého pohledu by měl asi pravdu. Pokud bychom se soustředili pouze na zabezpečení autorizace elektronických dokumentů, tak zde v řadě případů už dříve existovaly a dosud existují hojně využívané služby, které jsou založeny na více či méně proprietárních technologiích, jejichž právní rámec je dán smluvním vztahem mezi komunikujícími partnery. Typickým příkladem je oblast přímého bankovnictví. S ohledem na dobře zaběhané a osvědčené systémy lze očekávat, že řada takových služeb bude nadále paralelně koexistovat s aplikacemi založenými na platformě elektronického podpisu. Ty by namísto soupeření se stávajícími nástroji měly otevřít dveře elektronické výměně dokumentů v takových oblastech, kde předchozí přístupy už nestačily. Jedná se hlavně o styk se státními orgány a o „náhodné“ komunikace s předem nedeterminovanou množinou osob. Tady již vytváření ad hoc právních rámců pomocí účelových listinných smluv není schůdné. Další přínos jednotné legislativní úpravy lze spatřovat v kvalitativním zajištění nabízených služeb prostřednictvím státem stanovených a kontrolovaných podmínek provozu klíčových částí systému. Při vhodném způsobu uplatnění by taková síla měla v budoucnu chránit občany před masovými útoky ze strany hackerů, kteří budou stále lépe vybaveni detailními znalostmi slabin informačních systémů (viz *obr. 1*).

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] The European Electronic Signature Standardization Initiative, http://www.ict.etsi.org/EESSI_home.htm
[2] Menezes, A.-J., van Oorschot, P.-C., and Vanstone, S.-A.: Handbook of Applied Cryptography, CRC Press, 1996
[3] Ministerstvo informatiky, http://www.micr.cz
[4] Vyhláška č. 366/2001 Sb., platné znění viz [3]
[5] Zákon č. 227/2000 Sb., platné znění viz [3]
[6] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz

Elektronická komunikace pod dozorem

Internet jako komunikační médium má nedocenitelný význam v současném světě informačních technologií a samozřejmě v běžném životě. Nejčastěji využívanou službou na internetu je elektronická pošta. Přenášení zpráv touto cestou se jeví bezplatné a efektivní. Na ekonomických nákladech vynaložených na jednu přenesenou zprávu participuje nejen odesílatel, ale i příjemce a také poskytovatel přenosových služeb. Právě významné komunikační a distribuční vlastnosti e-mailu se stávají levným a účinným nástrojem marketingu firem a to formou hromadné distribuce zpráv ostatním stranám často vnucované i přes jejich nesouhlas. Podle statistiky představuje v ČR každý třetí e-mail nevyžádané obchodní sdělení. Šíření nevyžádaných obchodních sdělení ztrpčuje život uživatelům internetu. Rok 2005 by měl díky loňským iniciativám Ministerstva informatiky a Úřadu pro ochranu osobních údajů posílit důvěru uživatelů elektronické komunikace.

Ministerstvo informatiky v loňském roce připravilo zákon, jenž nabyl účinnosti 29. července a jehož cílem je omezit rozesílání nevyžádaných reklamních sdělení, například formou e-mailů nebo zpráv SMS. Zákonem č. 480/2004 Sb., o některých službách informační společnosti, byla vnesena do právního řádu České republiky směrnice Evropského parlamentu a Rady o elektronickém obchodu č. 2000/31/ES, s přihlédnutím ke směrnici o soukromí v elektronických komunikacích (2002/58/ES). Ta (v článku 5) zdůrazňuje povinnosti členských států EU zajistit důvěrný charakter sdělení přenášených informací veřejné komunikační sítě a veřejně dostupných elektronických služeb.
Základní myšlenkou zákona č. 480/2004 Sb., který patří podle odborníků na světě k nejtvrdším, je tedy posílení ochrany soukromí uživatele služby informační společnosti. Tím může být každá fyzická nebo právnická osoba. Zřejmá byla snaha zákonodárce docílit, aby uživatel nemusel vydávat žádné náklady na jemu doručená obchodní sdělení zasílaná elektronickou poštou, která si nevyžádal, a která jej ve svém důsledku jen obtěžují. V této souvislosti není důležitá samotná elektronická forma komunikace (obchodní sdělení může být učiněno i telefonem či faxem, ba i zprávou SMS).

Nad tím, aby zákon nebyl v běžném životě porušován, bdí Úřad pro ochranu osobních údajů (ÚOOÚ). Jeho působnost spočívá ve výkonu dozoru nad šířením obchodních sdělení v rámci podnikatelské činnosti; součástí výkonu dozoru je i prověřování podání týkajících se této činnosti a následné trestání. Uložená pokuta může dosáhnout až deseti milónů korun.

Pokud jde o institut souhlasu zákazníka, v návaznosti na nové znění příslušných ustanovení zákona o ochraně osobních údajů: pak tato jednoznačně deklarují, že souhlas subjektu údajů je projevem jeho vůle, tedy právním úkonem. Proto je možno očekávat i stejný přístup ÚOOÚ k prokazatelnosti souhlasu zákazníka s využitím elektronického kontaktu pro potřeby šíření obchodních sdělení, ve smyslu příslušných ustanovení zákona.

Za základní pravidlo pro komunikaci se zákazníkem (kterou tento zákon označuje jako šíření obchodních sdělení) lze považovat toto: i když souhlas byl udělen, musí být (dle téhož ustanovení) zákazníkovi při zaslání každé zprávy vytvořena možnost jednoduše a bez vynaložení nákladů souhlas odvolat. Obecně lze konstatovat, že i když je zákon o některých službách informační společnosti svou jednoznačnou preferencí metody „opt-in" pro komunikaci se zákazníkem poněkud přísnější — v porovnání s vymezením tohoto rámce v právu ES – zákonodárce tím dal všem subjektům působícím v této oblasti jednoznačně najevo svou vůli, kterou hodlá prosazovat také Úřad pro ochranu osobních údajů.

A ten v souvislosti s novými kompetencemi upozorňuje, že nelze zobecňovat problém v tom smyslu, že se jedná o postihování spamu jako takového. V tomto duchu vedl i řadu jednání se zástupci Ministerstva informatiky, představiteli reklamní sféry i právníky specializujícími se na uvedenou problematiku. Také upozorňuje subjekty, které by měly tendenci jednat bez ohledu na přijaté zákonné opatření, že bude uplatňovat sankční postihy, k nimiž je zákonem zmocněn. V zájmu dobré informovanosti veřejnosti a zjednodušení možnosti podávat ÚOOÚ stížnosti byla zřízena na jeho webových stránkách samostatná rubrika (http://www.uoou.cz/spam.php3).

Noh