VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská

Doc. Ing. Vladimír Smejkal, CSc.

ELEKTRONICKÝ PODPIS JAKO NÁSTROJ PRO ZVÝŠENÍ BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

ELECTRONIC SIGNATURE AS A TOOL OF IMPROVING THE INFORMATION SYSTEMS SECURITY

TEZE PŘEDNÁŠKY K PROFESORSKÉMU JMENOVACÍMU ŘÍZENÍ

OBOR: ODVĚTVOVÁ EKONOMIKA A MANAGEMENT

VUTIUM

BRNO 2003

KLÍČOVÁ SLOVA

bezpečnost informačních a telekomunikačních systémů, identifikace, autentizace, certifikát, elektronický podpis, digitální podpis, zákon o elektronickém podpisu, PKI (infrastruktura veřejných klíčů), bezpečnostní management, výuka bezpečnosti

KEY WORDS

Information and Communication Systems Security, Identification, Authentication, Certificate, Electronic Signature, Digital Signature, Electronic Signature Act, PKI (Public Key Infrastructure), Security Management, Education of the Security

ISBN 80-214-2447-8

ISSN 1213-418X

1 OBSAH

2 PŘEDSTAVENÍ AUTORA

Doc. Ing. Vladimír SMEJKAL, CSc. (*1955) je vysokoškolským učitelem, soudním znalcem a odborníkem na management informačních systémů, včetně jejich bezpečnostních a právních aspektů.

V letech 1979 až 1992 pracoval na ústředních orgánech státní správy a moci. Profesně se nejprve zabýval řízením výpočetních středisek, následně výzkumem a vývojem v oblasti umělé inteligence, poté právní informatice a organizaci a řízení v justici. Po získání doplňkového právnického vzdělání se stále více věnoval otázkám právních aspektů informatiky, zejména ve vztahu k trestné činnosti v podobě počítačové kriminality, přičemž v této oblasti začal rovněž působit pedagogicky a podílel se na výzkumné činnosti. Je rovněž odborníkem v oblasti bezpečnosti organizací, zejména v oblasti bezpečnosti informačních systémů, a podílel se na vyšetřování mnoha závažných trestných činů spáchaných v souvislosti s moderními informačními technologiemi zejména v oblasti ekonomiky a financí.

V roce 1997 se habilitoval na MU v Brně jako docent mezioborovou habilitační prací propojující obory práva a informatiky „Současný stav počítačové kriminality a její další perspektivy“. Nyní přednáší problematiku právních a bezpečnostních aspektů informačních systémů a Internetu na Vysoké škole ekonomické v Praze a na Vysokém učení technickém v Brně a vede nebo oponuje diplomové, rigorózní a doktorandské práce i na jiných vysokých školách. Je školitelem doktorandského studia na obou uvedených vysokých školách, členem komisí pro obhajoby disertačních prací a členem vědecké rady FP VUT.

V roce 1986 byl ministrem spravedlnosti ČSR jmenován soudním znalcem v oborech ekonomika a kybernetika, v roce 1995 byl jmenován ministrem spravedlnosti ČR soudním znalcem v dalších oborech, a to kriminalistika – ochrana dat a autorské právo.

Je autorem a spoluautorem řady knih („Počítačové právo“ – C.H.Beck 1995, „Internet a paragrafy“ – GRADA 1999 a 2001, „Právo informačních a telekomunikačních systémů“ – C.H.Beck 2001, „Řízení rizik“ – GRADA 2003, „Elektronický podpis“ – GRADA, v tisku, „Computer Law in the Czech Republic“ – Kluwer Law International, v tisku), skript a mnoha mezioborových článků z oblasti informatiky, práva a organizace a řízení.

Je členem představenstva Společnosti pro kriminalistiku, členem redakčních rad, spolupracovníkem a pravidelným přispěvatelem mnoha odborných periodik (Data Security Management, e-Biz, CHIP, INSIDE, Hospodářské noviny, Právní rozhledy, Právní rádce, Softwarové noviny, Network Communication apod.). Vystupuje na odborných konferencích u nás i v zahraničí (Francie, Rakousko, Itálie, Slovensko).

Otázkám spojeným s řízením podniků i nevýrobních organizací se zaměřením na budování a využívání informačních systémů, včetně jejich výkonnosti, efektivnosti a bezpečnosti, se věnuje dlouhodobě od roku 1980 doposud, a to včetně praktických aplikací v řadě bank a podniků. Nyní působí výlučně jako vysokoškolský učitel, nezávislý expert a soudní znalec, především v oboru ekonomiky a managementu, a to v oblasti řízení rizik, práva a bezpečnosti informačních systémů, počítačové kriminality a dalších aspektů informačních systémů.

Jako předseda subkomise pro právo informačních systémů Legislativní rady vlády České republiky se podílí na legislativních pracích v ČR v oblasti informatiky. Významný je jeho podíl na zákonu o elektronickém podpisu a na další české legislativě týkající se především elektronické komunikace. Působí rovněž v právní sekci České společnosti pro systémovou integraci a v dozorčí radě České asociace kompetitivních komunikací. Je členem poradního sboru předsedy Úřadu pro ochranu osobních údajů a členem kolegia ministra informatiky.

3 ÚVOD

Spis obsahuje teze přednášky k profesorskému jmenovacímu řízení, která je – v souladu se stanoviskem hodnotící komise – koncipována jako popis problematiky elektronického podpisu představujícího významný nástroj pro zvyšování bezpečnosti informačních systémů. Je to předmět autorova dlouhodobého teoretického i praktického zájmu, a to jak v rámci vědecko-výzkumné činnosti a legislativních projektů (autor byl hlavním zpracovatelem návrhu zákona o elektronickém podpisu a souvisejících předpisů),[1] tak v rámci konkrétních otázek spojených se zaváděním a užíváním tohoto autentizačního nástroje. V závěru díla je popsána koncepce vědecké práce a výuky v oblasti bezpečnosti a ochrany dat v informačních a telekomunikačních systémech.

Elektronický podpis představuje dnes jeden z nejaktuálnějších nástrojů identifikace a autentizace a je tedy jedním ze základních stavebních prvků při vytváření a užívání informačních a telekomunikačních systémů (dále také jen ITS). Přitom je třena zdůraznit, že elektronický podpis není pouze technologickým nástrojem na bázi kryptografie, ale má svůj rozměr legislativně-právní a organizačně-administrativní. Z hlediska jeho začlenění do struktury vědních oborů můžeme tedy konstatovat, že elektronický podpis je typickou aplikací mezioborového přístupu k problematice bezpečnosti a ochrany dat, jež je dnes tvořena řadou disciplín základního i aplikovaného výzkumu z oblasti přírodních věd (zejména matematika, statistika a informatika), technických věd (zejména, ale nejen elektrotechnika a kybernetika), jakož i věd společenských (právní vědy, ekonomika a management).

Následující text se proto nejprve věnuje popisu elektronického podpisu z hlediska jeho principů, užívání v oblasti identifikačních a autentizačních nástrojů, jakož i hlediska právních aspektů a souvislostí. Na výklad této konkrétní, vysoce aktuální problematiky, navazuje část obecná, ve které autor uvádí koncepci vědecké práce a výuky v daném oboru.

4 BEZPEČNOSTNÍ ASPEKTY INFORMAČNÍCH SYSTÉMŮ

4.1 LIMITY E-OBCHODU A E-GOVERNMENTU

Jedním z nejaktuálnějších aspektů vytváření a užívání informačních a telekomunikačních systémů, a to nejen v souvislosti s dálkovým přístupem, je bezpečnost a ochrana dat. Obecně se hovoří o tom, že další rozvoj elektronického obchodu a elektronické veřejné správy má dnes tyto hlavní limity:

1. dostupnost dálkového přenosu dat, tj. cena a rychlost připojení k Internetu;
2. právní, celní a daňové bariéry související s přeshraniční obchodem, resp. legislativní bariéry přeměny veřejné správy na e-government;
3. nedostatečná bezpečnost ITS, především při komunikaci prostřednictvím Internetu, ale nejen zde.[2]

---

[1] Smejkal, V., Mates, P.: Návrh zákona o elektronickém podpisu včetně předkládací a důvodové zprávy a vypořádání připomínkovacího řízení. Poslanecká sněmovna Parlamentu ČR, Praha 1999 – 2000 a Smejkal, V., Kodl, J., Mates, P.: Návrh nařízení vlády k provedení zákona o elektronickém podpisu včetně důvodové zprávy. Úřad vlády ČR, Praha 2001.

[2] Viz např. Smejkal, V.: Trendy ve zvyšování bezpečnosti a odolnost banky v internetovém prostředí. Sborník konference „Bankovní dny“, Institute for International Research, Praha 18.-19.9.2001.

Důsledkem těchto limitů je pohyb v začarovaném kruhu: málo uživatelů = málo aplikací a naopak. Proto je zvyšování bezpečnosti ITS jedním z nejnaléhavějších úkolů managementu vývojářů, výrobců, provozovatelů i uživatelů.

4.2 BEZPEČNOST ITS V KOMPLEXNÍM POJETÍ

Bezpečnost ITS můžeme chápat jako:

- **cíl**, kterého je třeba dosáhnout (ideální stav);
- **nástroj** k dosažení uvedeného cíle.

Pokud budeme chápat bezpečnost jako cíl, musíme mít k dispozici nějakou metriku, tj. kritérium, které nám řekne, od kterého okamžiku je ITS bezpečný, resp. jaká je úroveň jeho zabezpečení. (Proto někteří autoři dávají přednost pojmu „zabezpečený" a mluví o třídách zabezpečení systému.) Takovou metrikou je obvykle nějaká norma či standard, který říká obvykle věty typu „*Je-li vybaven ITS tímto a tímto, jedná se o bezpečný systém kategorie (třídy) XYZ.*" nebo jinak „*Chcete-li zabezpečit systém tak, aby splňoval požadavky na bezpečnost stanovené úrovně (a použít pro následné ověření příslušná kritéria pro hodnocení bezpečnosti ITS), musíte udělat toto a toto.*" Příkladem jedné z mnoha obecných definic bezpečnosti informací je tato:

Bezpečnost informací je charakterizována jako zachování:

a) důvěrnosti – zajištění toho, aby informace byla dostupná pouze osobám s oprávněným přístupem,

b) integrity – zabezpečení správnosti a kompletnosti informací a metod zpracování,

c) dostupnosti – zajištění toho,aby informace a s nimi spjatá aktiva byly přístupné oprávněným (autorizovaným) uživatelům podle jejich potřeby.

Někdy bývá součástí tohoto „triumvirátu" i požadavek čtvrtý – neodmítnutelnost (odpovědnosti), také nepopiratelnost, neboli zajištění toho, aby byly k dispozici dostatečné důkazní prostředky o provedení určité operace, která může mít charakter právního úkonu (např. jako důsledek přijetí zprávy, podepsání dokumentu apod.), ale také může být nelegální akcí, jejíž uskutečnění může ohrozit chod či existenci celé organizace (kriminální čin spočívající ve změně údajů v počítačové databázi – např. záměna čísla účtu v převodním příkazu).[3]

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat v podobě pravidel, natrénovaných postupů, procedur, organizační struktury a programových funkcí.

Příkladem může být požadavek na implementaci určité funkce např. tohoto typu: „*Zabezpečený ITS vyžaduje, aby se uživatelé sami identifikovali před zahájením provádění jakékoliv činnosti, která je ITS zprostředkovávána. ITS by měla používat chráněný mechanismus k ověření totožnosti*

[3] Více viz např. Smejkal, V.: Lumpáren se nezbavíme. Prognóza dalšího vývoje v oblasti informační a informatické kriminality. (We Will not Get Rid of the Dirty Business. A prognosis of the future development of information technology crime.) In: Vize informační bezpečnosti 2002 – 2003. Data Security Management, TATE International, s.r.o., Praha 2002, s. 50 – 53, Smejkal, V.: Informatická a počítačová kriminalita. Pojistné rozpravy, 2002, č. 12, s. 142 – 176 nebo Smejkal, V.: Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, II., 2003, č. 6, s. 161 – 167.

uživatele a chránit autentizační údaje, aby nebyly přístupny neoprávněnému uživateli.“ (Požadavek pro třídu zabezpečení C1 podle TCSEC).[4]

Proč hovoříme v souvislosti s budováním bezpečných ITS a jejich bezpečným užíváním o určitém manažerském problému? Protože je v této oblasti mnoho co dohánět.

Bezpečnost informačního systému organizace (podniku, orgánu veřejné správy apod.) je pouze jednou ze složek celkové bezpečnosti tohoto subjektu. Bývá proto tendence redukovat i složky bezpečnosti ITS organizace pouze na problematiku „čistého“ informačního a telekomunikačního systému, tj. hardware a software. Tím dochází k ignorování mnoha dalších hrozeb, nejsou činěna protiopatření a na incidenty mimo očekávanou oblast není organizace připravena.[5]

Bezpečnost informačních systémů organizace je třeba zajistit z hlediska všech složek, jež tvoří současně oblasti celkové bezpečnosti organizace:

- personální bezpečnost
- administrativní bezpečnost
- objektová bezpečnost
- hardwarová bezpečnost
- softwarová bezpečnost
- datová bezpečnost
- komunikační bezpečnost.

Jakým způsobem budou tyto faktory zohledněny při budování bezpečné organizace (podniku) a jejího bezpečného informačního a telekomunikačního systému, to je záležitostí komplexní bezpečnostní koncepce podniku a její realizace. (Jde o třetí krok v procesu budování bezpečného ITS, po analýze rizik a z toho vyplývajícího formulování bezpečnostní politiky.)[6]

Bezpečnostní koncepce ITS je hlavním řídícím dokumentem subjektu pro definování systému řízení bezpečnosti ITS. Kromě popisu systému řízení bezpečnosti ITS, obsahuje především popis existujících a zamýšlených bezpečnostních projektů a opatření. Jedná se tedy o hierarchickou soustavu tohoto typu – viz obr. 1. Proces zajišťování bezpečnosti ITS musí současně zahrnovat i vyhodnocování bezpečnostních opatření z hlediska dalších základních charakteristik ITS, jako jsou výkonnost, ekonomická efektivnost, spolehlivost apod., neboť jde o soustavu ukazatelů, které se značně vzájemně ovlivňují. Přitom požadavky na snižování nákladů na provoz ITS jsou obvykle v přímém rozporu s požadavky na zvyšování jeho bezpečnosti a spolehlivosti.[7] Především v podmínkách malých a středních podniků je nákladová stránka považována za rozhodující, ačkoliv správně provedená riziková analýza by odhalila, že tím dochází k neúměrnému ohrožení podniku, jde tedy o šetření na nesprávném místě.[8]

---

[4] TCSEC – Kritéria hodnocení bezpečnosti počítačových systémů. BEN, Praha 1994.

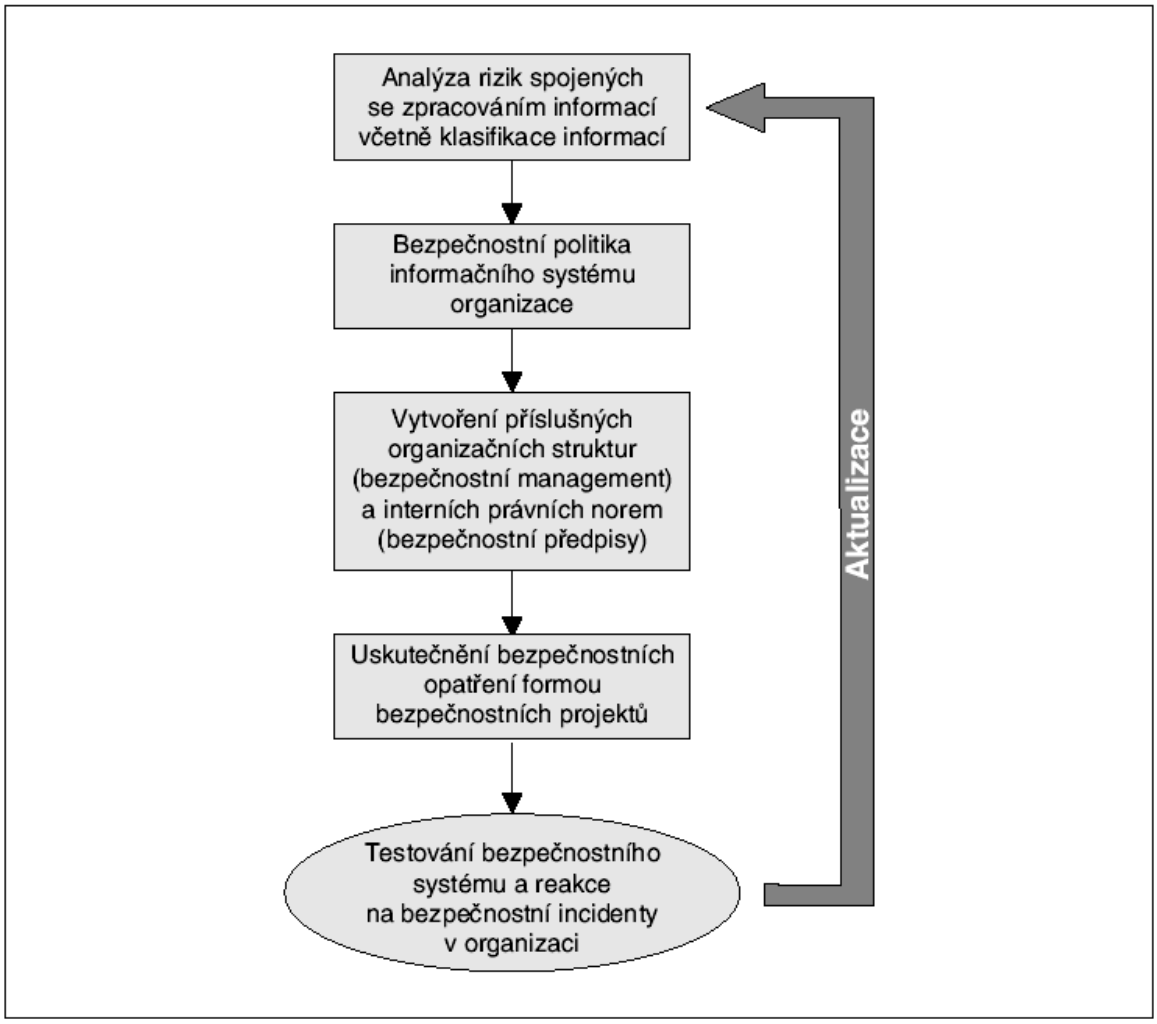
[5] K této problematice viz např. Smejkal, V., Rais, K.: Řízení rizik. 1. vydání. GRADA, Praha 2003.

[6] Viz např. Smejkal, V.: Ochrana osob, organizací a informačních systémů. Právní rádce, 2001, č.10, s. 8 –15

[7] K charakteristikám ITS viz např. Rais, K., Smejkal, V. a kol.: Řízení výpočetních středisek na vysokých školách - třetí etapa dílčího úkolu SPEV 90910110, Brno 1985; Rais, K., Smejkal, V.: Vybrané charakteristiky počítačových systémů a jejich hodnocení. Výzkumná zpráva SPEV 909334503/052 "Informační systémy a moderní metody řízení v odvětví kultury a jejich metodologie". UISK, Praha 1987; Rais, K., Smejkal, V.: Evaluation of Terminal System Performance. Sborník Evropského kongresu o simulaci (European Congress on Simulation). Praha, 21.-25.12.1987, str. 130 – 134.

[8] Opakované zkušenosti autora z bezpečnostních analýz a projektů v řadě podniků a jiných organizací.

Je vidět, že bezpečnost ITS není jeden cíl, kterého lze dosáhnout stejně, jako vrcholku hory, ale nepřetržitý proces definování cílů, provádění opatření, vyhodnocování, korekce cílů a opatření atd. Přitom prakticky vždy, když budeme hovořit o bezpečnosti či připravovat určitá bezpečnostní opatření, setkáme se se základními bezpečnostními funkcemi či procesy, jakými jsou identifikace a autentizace.



Obr. 1 – Proces budování a řízení bezpečnosti organizace

5 IDENTIFIKACE A AUTENTIZACE

Jednou z klíčových otázek bezpečného zpracování dat (případně obecně řečeno bezpečného provádění jakýchkoliv úkonů člověkem) je otázka „určení osoby, která takový úkon učinila“, tedy identifikace a s tím související autentizace neboli ověřování totožnosti, tj. že subjekt je tím, za koho se prostřednictvím této identity vydává.

Jedná se o dva různé pojmy a dva různé okamžiky v určitém bezpečnostním procesu:

1. *Identifikací* rozumíme rozpoznání entity systémem, a to na základě určitého identifikátoru (datové položky), která je spojena s určitou osobou, reprezentuje jeho identitu a může být známa

jiným osobám. Typickým příkladem je jméno a příjmení, případně další identifikátory, odstraňující zaměnitelnost. Právně je identifikace určení osoby, která učinila určitý úkon.

Příklad: identifikace spočívá v uvedení jména a příjmení v e-mailu, zaslaném v normální, znakové podobě příjemci. Ten si spojí zprávu s uvedenou osobou, ale nemá jistotu, zda skutečně je osoba uvedená v identifikátoru odesílatelem (signatářem).

2. *Autentizace* znamená ověřování proklamované identity subjektu. Problém autentizace řešilo lidstvo od toho okamžiku, kdy byla poprvé určena zpráva vzdáleným příjemcům. Prvními prostředky autentizace byli svědkové (osoby zaručující se za pravost zprávy), později převzaly tuto úlohu autentizační předměty (nejčastěji prsten, ale třeba i zbraň). Také k prvním písemným projevům (např. sdělením vládce vzdálené provincii) se vyjadřovali svědci a až později se objevila autentizace pečetí či podpisem, tedy nikoliv již samostatnou věcí, ale něčím, co tvořilo součást dokumentu.

Dnes se identifikace u papírových dokumentů provádí nejčastěji uvedením jména a příjmení podepisující osoby a autentizace podpisem, který může srovnat příjemce s jemu známým podpisovým vzorem. Pravost podpisu by pak v případě sporu o autorství dokumentu mohla být prokazována písmoznalecky posudkem soudního znalce. Vyšší stupeň autentizace podepsaného dokumentu se provádí podpisem před svědky (typicky u závěti), ověřením totožnosti pověřenou osobou (advokátem); vrcholem autentizační hierarchie je u listin vidimace a legalizace formou úředně ověřeného podpisu[9] nebo notářského zápisu.[10]

Podle § 40 odst. 4 občanského zákoníku je písemná forma zachována také tehdy, když je učiněna elektronickými prostředky. Současně je však třeba, aby byly splněny dvě podmínky: musí jít o takové prostředky, které umožňují zachycení obsahu právního úkonu, a dále určení osoby, která takový úkon učinila. Druhá podmínka spočívá tedy opět v procesu identifikace a autentizace osoby.

V oblasti ITS je otázka ověřování pravosti dokumentů a podpisů poněkud složitější, ale pouze zdánlivě. Záleží to také mj. na formě zpracovaných dat, tj. zda se jedná o obrazovou nebo znakovou informaci.

Rozlišovací schopnost stávajících prostředků pro pořízení digitální podoby (obrazu, faksimile) dokumentu je dnes na tak dostatečné úrovni, aby bylo možno zkoumat, zda podpis na původně papírovém dokumentu, jehož obraz je uložen např. na CD disku, učinila daná osoba. Jediným momentem, který by mohl vést ke zpochybnění pravosti podpisu (nebo jiné části dokumentu) je námitka, že při digitalizaci, tj. pořizování faksimile a jeho ukládání na disk, došlo k úpravě obsahu ukládaného dokumentu. Tuto námitku nelze samozřejmě absolutně odmítnout, nicméně lze jinými důkazními prostředky (výpověďmi svědků, technickým provedením snímacího zařízení, způsobem uložení digitalizovaných dat na nosiči informací, smlouvou se zákazníky, jimž je služba digitalizace poskytována) posílit důkazní hodnotu digitalizovaných dokumentů. Vhodné též je, aby byl používán takový program, který může v maximální možné míře zachytit, že došlo k nějakému zásahu do elektronicky pořizovaného záznamu (procesu digitalizace) – nejlépe formou vytváření auditní stopy o procesech probíhajících v zařízení při jeho provozu. Uvedený postup přichází v úvahu tedy tam, kde bude digitalizovaná forma vytvářena převodem z papírové podoby – v dnešní době dochází k hromadnému převádění některých archivů do elektronické podoby (přičemž

[9] Notářem podle notářského řádu nebo pověřeným pracovním orgánu veřejné správy podle zákona č. 41/1993 Sb., o ověřování shody opisů nebo kopie s listinou a o ověřování pravosti podpisu obecními úřady a o vydávání potvrzení orgány obcí a okresními úřady, ve znění pozdějších předpisů

[10] Viz zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů.

zkušenosti ze záplav roku 2002 zřejmě tento proces ještě urychlí). Podle publikovaného názoru[11] lze většinu dokumentů, které vznikají nebo jsou součástí evidencí vedených subjekty soukromého práva, převést na digitální obrazový záznam; rovněž v oblasti veřejnoprávní je okruh stále ještě „nedigitalizovatelných“ dokumentů omezený.

Jestliže však půjde o přímý převod z elektronické analogové podoby na digitalizovanou (digitalizace hudby, zvuku, obrazu) nebo o zápis provedený primárně sice elektronicky, leč ve znakové podobě (na klávesnici počítače), je možnost identifikace a především autentizace osoby, která má být s dokumentem ztotožněna (činí určitý úkon) omezená. Zejména pokud se tak činí na dálku prostřednictvím prostředků umožňující dálkový přístup ke zpracování dat, např. pomocí Internetu. Pak by musely být soubory obsahující texty v elektronické podobě opatřeny zvláštním mechanismem, umožňujícím ověření totožnosti podepsané osoby, a to výlučně z těchto elektronických dat, případně ve spojení s jinými daty, ale tak, aniž by muselo dojít k fyzickému kontaktu s podepsanou osobou. Jedině tak má tento způsob význam pro on-line dálkové zpracování dat (např. zmíněný e-obchod či e-government).

Autentizaci uživatele ITS lze provést na základě skutečnosti, že:

- uživatel něco ví (heslo);
- uživatel něco má (autentizační předmět – kalkulátor, čipovou kartu, mobilní telefon);
- uživatel má nějaké vlastnosti, systémem rozpoznatelné na bázi biometrie – fyziologické vlastnosti (otisky prstů, struktury oční duhovky, tvar obličeje nebo jeho části – např. ucha, rtů, geometrie prstu a ruky apod.) nebo chování – dynamika určitého projevu (stisku klávesy, psaní rukou, chůze) nebo analýza hlasu.

Pokud by mělo být upuštěno od dokazování pravosti dokumentu i podpisu samého nějakými dalšími podpůrnými prostředky, což je při dálkovém přenosu dat nezbytné, pak dnes přichází v úvahu pouze jedna alternativa: identifikace a autentizace se při tomto způsobu zpracování dat zajišťuje především tzv. elektronickým podpisem.[12]

Nebylo tomu tak od samého počátku – typicky např. v oblasti finančních institucí. Autentizace prošla vývojem od osobní autentizace (klient se dostavil do banky), přes autentizaci podpisem (podpisovým vzorem), až po autentizaci např. zavoláním do banky (sofistikovanější varianta používala volání opačným směrem, tzv. call back), potvrzujícím obsah doručeného dokumentu. První varianta byla nepohodlná, druhá a třetí snadno zneužitelná. Hledaly se proto různé jiné způsoby zvyšující bezpečnost autentizace, např. používání hesel při telefonickém styku, což některé banky používají u tzv. telefonbankingu doposud. Zde ale dochází k rozporu mezi pohodlím klientů a úrovní zabezpečení: délka a složitost klíčů je nutným požadavkem pro dostatečnou bezpečnost proti útoku na heslo tzv. hrubou silou nebo logickým útokem (odhadem). Navíc stále stejné nebo nepříliš variabilní heslo (například dnes stále používaná varianta sdělení některé z číslic rodného čísla) je snadno monitorovatelné a následně použitelné útočníkem, vydávajícím se za klienta. Institut jednorázových hesel, který je použitelný např. v diplomacii, zcela jistě není ideálním nástrojem pro podnikatele, denně komunikujícím s jednou či více bankami.

Hledal se tedy autentizační prostředek, který by splňoval následující požadavky:

a) pracoval na principu neopakování autentizačních dat (hesla);
b) byl snadno použitelný;

---

[11] Mates, P., Smejkal, V.: Dokumenty budoucnosti, Data Security Management, II., 5/1998, str. 34 a násl.

[12] Mates, P., Smejkal, V.: Elektronické podpisy. Právní rádce, VII., 1999, č.9, s. 17; Grant, G.L.: Understanding Digital Signatures. McGraw – Hill, USA 1997; Menzel, T.: Elektronische Signaturen. Verlag Österreich, Wien, 2000.

c) byl chráněný proti neoprávněnému použití;

d) poskytoval vysokou záruku nezneužitelnosti (neprolomitelnosti).

Prvními pomůckami, požadujícími provedení autentizace, byly platební či jiné karty s čísly PIN (dnes se s „PINy“ setkáme skoro na každém kroku) nebo autentizační předměty, provádějící identifikaci a autentizaci prostřednictvím určité tajné informace. Najdeme je všude, kde jde o nějaké přístupové oprávnění – heslo k počítači, číselný kód na trezor, dotyková paměť u immobilizéru v automobilu nebo u počítače (jako přívěsky ke klíčům, prsteny – tzv. touch memory atp., obsahující autentizační informaci). Zde ovšem chybí důležité ujištění, že jde skutečně o oprávněnou osobu a nikoliv o delikventa, který odcizil klíče i s immobilizérem nebo odpozoroval či uhádl číselnou kombinaci.

Jiným druhem autentizačního prostředku, navíc použitelným obecně i pro telefonbanking, faxbanking i internetbanking, jsou tzv. optické klíče[13] neboli autentizační kalkulátory. Jde v podstatě o zařízení, do kterého se přistupuje prostřednictvím další utajené informace – PIN uživatele, a které obsahuje identifikaci klienta nebo účtu. Tento kalkulátor má umožnit klientům bez jakéhokoliv dalšího prokazování disponovat se svým účtem na kterékoliv pobočce banky – osobně nebo na dálku. Funguje tak, že banka sdělí klientovi nějaké, náhodně generované číslo. Ten toto číslo zadá do zařízení, které s pomocí tajné informace v něm uložené, klientovi neznámé, spočítá jiné číslo. Toto číslo sdělí klient zaměstnanci banky na „druhé straně drátu“ nebo přímo bankovnímu počítači přes Internet. Ten porovná spočtené číslo s číslem, které je spočteno bankovním počítačem a pokud čísla souhlasí, lze konstatovat, že osoba je tím, kdo je uveden ve zprávě (kdo se za klienta vydává). V případě dálkového spojení prostřednictvím Internetu může fungovat optický klíč dokonce jako obousměrný autentizační nástroj, který funguje způsobem „výzva – odpověď“ jak od banky ke klientovi, tak od klienta k bance, a ověřuje pro každou ze stran věrohodnost protistrany.

Elektronické dokumenty a jejich dálkový přenos, nastolily otázku autentičnosti účastníků telekomunikace a prokazování pravosti dokumentů a podpisů s vysokou naléhavostí. Je totiž třeba:

1. doručit data k příjemci, aniž by byla útočníkem poškozena či modifikována, eventuálně také je zabezpečit proti prozrazení (odposlechu);

2. prokázat, že odesílatelem je skutečně odesílatel;

3. zajistit, aby příjemce nemohl popřít doručení dat, případně odesílatel jejich odeslání.

Ad 1) jde o zajištění ochrany proti neoprávněné modifikaci (zajištění integrity dat) a proti odposlechu (zajištění utajení dat, obvykle šifrováním).

Ad 2) jde o identifikaci a autentizaci odesílatele.

Ad 3) jde o dosažení tzv. nepopiratelnosti, přičemž nepopiratelnost u odesílatele je zajištěna splněním požadavku ad 2., zatímco u doručitele musí být řešena organizačním opatřením, např. spočívajícím v odeslání odpovědi opatřené rovněž autentizačními atributy.

Metody, které se volí pro umožnění bezpečné identifikace a autentizace odesílatele, jakož i pro zajištění integrity dat, jsou různé: například banky používají k potvrzení pravosti platebních příkazů předávaných na magnetických médiích papírové dokumenty, tzv. konfirmační dopisy. Klienti některých bank, kteří chtějí podávat příkazy telefonicky či faxem, musí disponovat kromě identifikace jménem či číslem účtu také heslem.

[13] V některých verzích je výstupní signál z tohoto přístroje (velikosti kalkulačky) snímán do terminálu pobočky, proto optický klíč.

Při rozsáhlejších či významnějších přenosech dat potřebujeme ovšem mechanismus, který poskytne větší jistotu pro zúčastněné subjekty. Není totiž problém, zejména při používání telefonického spojení prostřednictvím veřejné telefonní sítě, ale i prostřednictvím pronajatých telekomunikačních okruhů, aby se prakticky kdokoliv kdykoliv připojil k přenosům dat, monitoroval je a takto zjistil potřebná hesla nebo jiné údaje. Na druhou stranu použití tohoto mechanismu musí být jednoduché (uživatelsky jednoduché), rychlé (bez nároků na výpočetní mohutnost systému) a bezpečné (neprolomitelné). Takovým nástrojem je dnes elektronický podpis.

6 ELEKTRONICKÝ PODPIS

6.1 ELEKTRONICKÝ PODPIS A VLASTNORUČNÍ PODPIS

Elektronický podpis je – stejně jako „ruční“ (vlastnoruční) podpis – výsledkem nějakého procesu, vyplývajícího z rozhodnutí podepisující osoby, jehož úkolem je stvrdit vůli této osoby, případně její identitu.

Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují ale i aktuální vnější a vnitřní podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen. Zkoumání pravosti písma (podpisu), které je zaměřeno na grafickou stránku směřující k identifikaci pisatele, je prováděno pomocí různých metod, přičemž za základní metodu je považována metoda pozorování, dále pak to jsou metody analytická, syntetická, komparační a grafometrická.[14] Jak u podepisování, tak u zkoumání pravosti (ověřování) podpisu jde tedy o procesy převážně subjektivního charakteru, v nichž se promítají obecné a individuální vlastnosti zúčastněných osob.

Elektronický podpis je naproti tomu od okamžiku „odstartování“ podepisování, tedy od okamžiku učinění rozhodnutí podepisující osoby až po okamžik ověření pravosti podpisu, objektivním výsledkem technologického, na zvláštnostech zúčastněných osob nebo situace nezávislého, procesu. Je výsledkem aplikace určité, pro podepisující osobu charakteristické vlastnosti (tajné informace) na podepisovaný text; jedná se tedy – na rozdíl od ručního podpisu – o podpis proměnný a bez znalosti soukromého klíče nevytvořitelný (což vyplývá z jeho principů).

Jak si ukážeme dále, možnost zneužití elektronického podpisu není větší, než podpisu ručního, zatímco možnost ověření pravosti elektronického podpisu je daleko vyšší.

6.2 ELEKTRONICKÝ PODPIS A ZARUČENÝ ELEKTRONICKÝ PODPIS

Existují dva stupně elektronického podpisu: „obyčejný“ a „zaručený“. Zákon[15] i směrnice[16] o elektronickém podpisu říkají, že (obyčejným) *elektronickým podpisem jsou údaje v elektronické*

[14] Musil, J. a kol.: Kriminalistika. Praha, Naše vojsko 1994, s. 110-111

[15] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

[16] Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Citace (CELEX): 399L0093, publikováno v OJ L 013.

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. Neříkají nic o tom, jakou technologií mají být tato data vytvořena a jak se má postupovat při zmíněném ověření totožnosti. S „obyčejným“ elektronickým podpisem se proto můžeme dnes setkat např. v bankách při porovnávání podpisu na papíru s podpisovým vzorem, oskenovaným a uloženým v paměti počítače. Srovnání je ale pouze vizuální a záleží na momentální kondici podepisujícího i na schopnostech bankéře, aby odhalil, zda jde o padělek. Jde tedy o postup ryze subjektivní.

Naproti tomu tzv. *zaručený elektronický podpis* (dále také jen ZEP) přináší do světa podepisování zcela novou kvalitu. Jedná se o údaje, které jsou připojeny k obsahu elektronického dokumentu a které jsou vytvořeny zvláštním postupem, dnes nejčastěji s využitím kryptografických principů. ZEP umí vše, co vlastnoruční podpis na papíru, a navíc poskytuje řadu funkcí, které na papíře nemůžeme nikdy dosáhnout:

1. identifikuje původce podpisu (to znamená, že příjemce zprávy bezpečně ví, kdo je autorem či odesilatelem elektronické zprávy),

2. zaručuje nepopiratelnost (osoba nemůže popřít, že danou zprávu s daným obsahem vytvořila),

3. zaručuje integritu zprávy (příjemce má jistotu, že zpráva nebyla změněna), a to především proto, že:

4. podpis je vytvořen pomocí prostředků, které podepisující osoba může mít pod svou výhradní kontrolou.[17]

Pro tvorbu elektronického podpisu se dnes používá prakticky výlučně metoda *podpisu digitálního*, využívající existence dvou klíčů patřících podepisující osobě: soukromého a veřejného, tedy metoda na bázi asymetrické kryptografie. (V budoucnosti ale může zaručený elektronický podpis fungovat na základě zcela jiné, nově objevené metody.) Můžeme a musíme si proto vyložit princip, na kterém dnes technologicky realizujeme elektronický podpis, tedy metodu podpisu digitálního.

6.3 PRINCIP DIGITÁLNÍHO PODPISU

Mějme elektronický dokument v digitální podobě (dále také jen digitální dokument), což je libovolná posloupnost dat neboli – na nejnižší úrovni – libovolná posloupnost bitů. V zákonu o elektronickém podpisu tomuto pojmu odpovídá termín „datová zpráva. Digitálními dokumenty mohou být soubory textové, obrazové, zvukové atd., ale i počítačové programy, mapy nebo jednotlivé položky v databázi apod. (Můžeme proto podepsat i svůj program tak, aby bylo zřejmé, že je náš, že jsme jej vytvořili apod.) Ve všech případech jsou to ale „pouhé“ posloupnosti bitů – nul a jedniček. A protože posloupnost bitů můžeme chápat jako číslo, digitální dokument bude pro nás číslo. Většinou to bude opět velké číslo, třeba bude mít miliony číslic, ale na jeho podstatě to nic nemění.

Protože ale by práce s tak velkými čísly činila při požadavcích na rychlé zpracování elektronického podpisu problémy, prvním krokem při podepisování je jistá redukce tohoto čísla = celého dokumentu na jeho reprezentaci, tj. jiné, kratší číslo, které je nicméně vzhledem k obsahu dokumentu jednoznačné a má pevnou délku. Jedná se tedy o kryptografickou metodu tzv. hashování, kdy je pomocí jednocestné funkce převedeno ono velké číslo (obsah dokumentu) na

[17] Pomíjím poněkud spekulativní diskuse na téma, zda dnes můžeme mít vůbec nějaký technický prostředek na bázi výpočetní techniky, coby konglomerát hardware, software systémového a software aplikačního, absolutně pod kontrolou.

číslo kratší. Vstupem hashovací funkce H je datový soubor M (zpráva) o proměnné a prakticky neomezené délce, výstupem je hashovací hodnota H(M), tj. hodnota vzorku zprávy, která má konstantní délku, podle použitého algoritmu. (U nejrozšířenějšího algoritmu SHA-1 to je 160 bitů, ale dnes jsou v procesu návrhu funkce s výstupem delším: SHA-256, 384, 512 bitů.) Podstatné jsou vlastnosti této funkce, která musí být jednocestná a bezkolizní.[18]

Proces podepisování je analogický s podepisováním vlastnoručním. Místo papírového dokumentu máme k dispozici číslo, reprezentující digitální dokument, a místo podpisové schopnosti (uložené v mozku a vykonávané v důsledku vlastností těla resp. ruky) máme tajné podepisovací číslo, tj. privátní klíč. Určitým matematickým spojením, založeným na vlastnostech asymetrických kryptografických algoritmů, z těchto dvou čísel vzniká číslo nové, a tím je právě digitální podpis.

Algoritmem, který je nejčastěji používán pro digitální podpis, je známý algoritmus RSA.[19] Využití systému RSA vychází ze skutečnosti, že procesy šifrování a dešifrování jsou jeho případě reversibilní (inverzní). Základní model elektronického podpisu vlastnosti reversibility s výhodou využívá.

Také ověřování pravosti podpisu má svůj ekvivalent v klasickém ověřování vlastnoručního podpisu. Naším podpisovým vzorem pro ověření digitálního podpisu je opět číslo, které můžeme nazvat veřejným ověřovacím číslem (veřejným klíčem). Toto ověřovací číslo je sice pevně svázáno s číslem podepisovacím a může být dáno veřejně k dispozici, stejně jako podpisový vzor u ručního podpisu a podobně jako podpisový vzor, ani toto číslo nikomu nedává schopnost digitální podpis vytvářet, ale pouze ho ověřovat. (Zatímco existuje značná pravděpodobnost, že se někdo naučí napodobovat cizí podpis podle podpisového vzoru, možnost, že by se kdokoliv ze znalosti veřejného klíče propracoval ke klíči soukromému, je prakticky vyloučena.)[20]

6.4 INTEGRITA DOKUMENTU

Z výše uvedeného vyplývá, že digitální podpis je funkcí soukromého klíče (SK) a datové zprávy reprezentující obsah podepisovaného dokumentu (jeho hashe), což lze vyjádřit vzorcem takto:

$$\text{PODPIS} = f\,(g(\text{obsah}); \text{SK}).$$

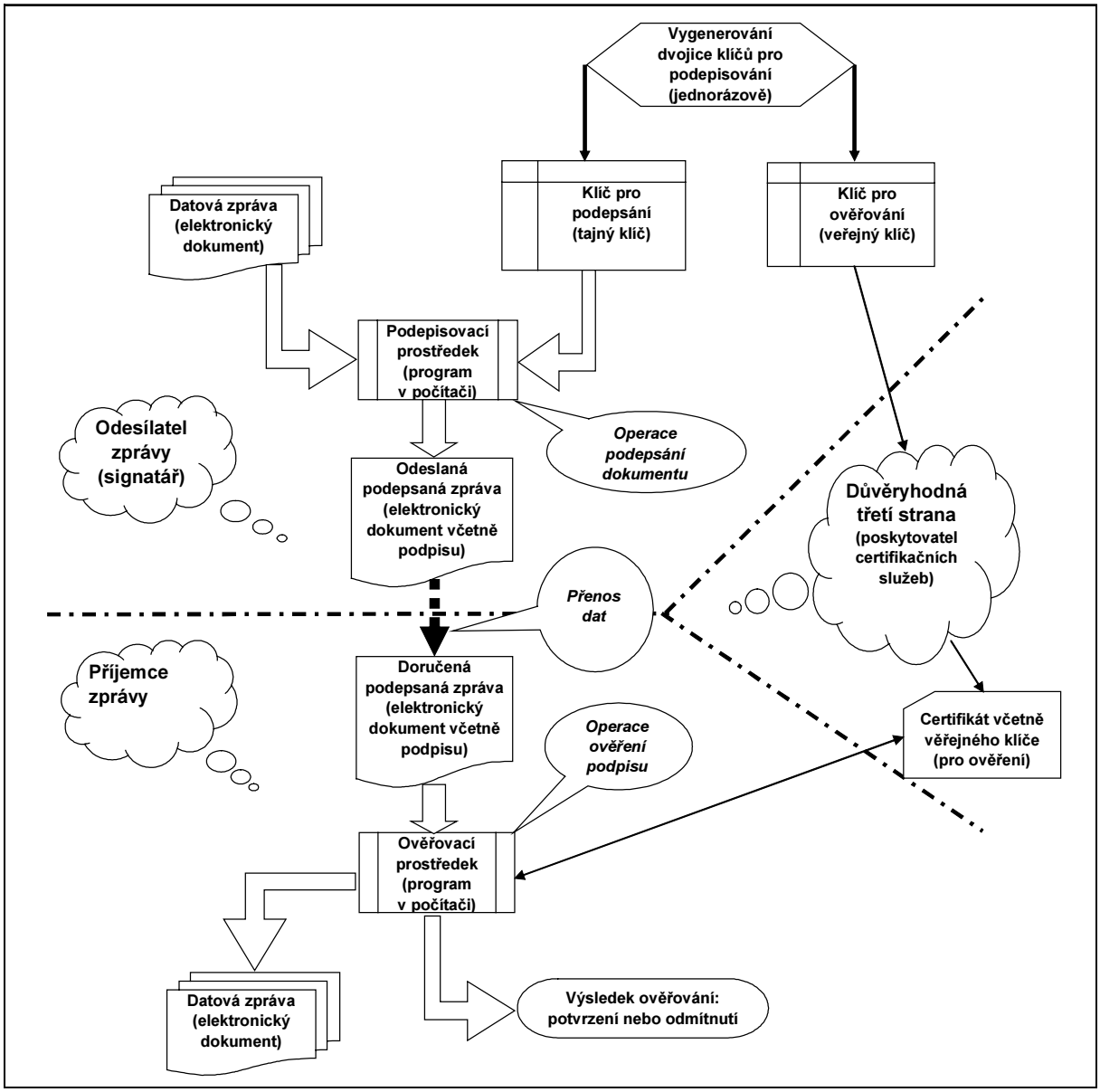
Digitální podpis má tedy vlastnost, kterou podpis na papíru nikdy nemůže zajistit: protože podpis je funkcí soukromého klíče a obsahu podepisovaného dokumentu, pak když se změní klíč nebo dokument, výsledek je pokaždé jiný. Jinými slovy, elektronický podpis je nepřenosný na jiný elektronický dokument, je tedy pro každý různý podepsaný dokument různý. (Soukromý klíč je přitom konstantní.) Použití elektronického podpisu na bázi podpisu digitálního tedy umožňuje

[18] Jednocestnost: je-li dáno M, je jednoduché vypočítat H(M); je-li dáno H(M), je velmi těžké (výpočetními prostředky prakticky neproveditelné) vypočítat M; je-li dáno M, je velmi těžké nalézt M´ tak, aby H(M) = H(M´). Odolnost proti kolizi: je velmi těžké nalézt jakékoliv různé M a M´ tak, aby H(M) = H(M´), tj. aby došlo k tzv. kolizi.

[19] http://www.rsasecurity.com

[20] K problematice faktorizace (nalezení všech prvočinitelů složeného čísla) při luštění algoritmu RSA, z hlediska potřebného času, výpočetní mohutnosti atd. – viz např. Silverman , R.D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. RSA Laboratories, April 2000 Bulletin #13 (Revised November 2001), http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html.

současně zjistit, zda došlo k nějakému zásahu do obsahu dokumentu po jeho podepsání, tedy kontroluje integritu elektronického dokumentu.[21]



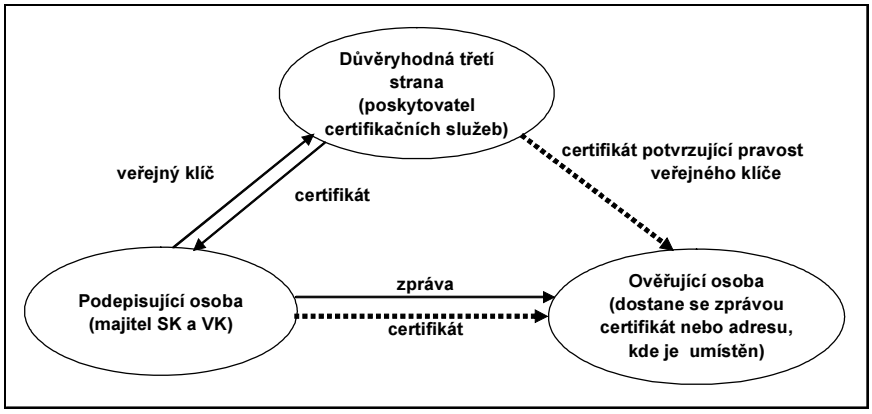
Obr. 2 – Proces podepisování a ověřování podpisu

6.5 CERTIFIKÁTY A POSKYTOVATELÉ CERTIFIKAČNÍCH SLUŽEB

Veřejný klíč může příjemce získat různými způsoby: dostane jej osobně od majitele, nebo je klíč někde veřejně k dispozici s uvedením, komu patří - obvykle na Internetu, případně existují řešení, která zabezpečenou cestou tyto veřejné klíče distribuují. Na Internetu ovšem nemáme vždy

[21] Pracuje se ale i na jiných metodách, např. verifikaci podpisu na bázi dynamické biometrie, kdy se porovnávají změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na a nad snímačem.

jistotu, že ten, kdo je označený jako majitel veřejného klíče, jím také skutečně je. Potřebujeme tedy někoho, kdo příjemci zaručí pravost veřejného klíče – *důvěryhodnou třetí stranu* – viz obr. č. 3.



Obr. 3 – Trojúhelník důvěry v elektronický podpis

Podle zákona[22] je touto stranou *poskytovatel certifikačních služeb*, což je soukromoprávní subjekt, poskytující službu spočívající v propojení fyzické osoby s jejím veřejným klíčem prostřednictvím tzv. *certifikátu*. Certifikátem zaručuje, že veřejný klíč patří opravdu tomu, kdo je označen jako jeho vlastník.

Certifikát je digitální dokument, v kterém jsou kromě jiného (například čísla certifikátu, doby platnosti od - do, ověřovací metody apod., podle druhu certifikátu) uvedeny zejména údaje, identifikující příslušnou osobu, a její veřejný ověřovací klíč. Tento digitální dokument je pak digitálně podepsán tzv. certifikační autoritou (podle zákona i dle směrnic ES *poskytovatelem certifikačních služeb,* dále také jen PCS)[23] a to dohromady dává žádaný podepsaný certifikát.

Dnes se používají především dva typy certifikátů, a to podle X.509[24] a PGP.[25] Můžeme se ale setkat i s certifikáty jiných formátů.

6.6 BEZPEČNOST ELEKTRONICKÉHO PODPISU

Vysoká bezpečnost zaručených elektronických podpisů vyplývá z použité podepisovací a ověřovací metody; dále je dána důvěryhodností poskytovatele certifikačních služeb, především tím, jak zodpovědně ověří pravdivost vztahu mezi veřejným klíčem a jeho majitelem; a konečně spolehlivostí oprávněné osoby, tj. tím jak udržuje svůj soukromý klíč (= podepisovací údaje) v tajnosti. Protože zaručený elektronický podpis je vázán na konkrétní fyzickou osobu, lze předpokládat, že každý si bude svůj soukromý klíč chránit „jako oko v hlavě“, podobně jako PIN ke kartě do bankomatu; jinak bude nést důsledky za zneužití svého podpisu.

---

[22] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

[23] angl. certification service provider (CSP), něm. Zertifizierungsdiensteanbieter (ZDA)

[24] ITU, dříve CCITT je International Telecommunication Union, jejíž sekce ITU Telecommunication Standardization Sector (ITU-T) vydává standardy se vztahem k telekomunikacím. Přehled viz http://www.itu.int/rec/recommendation.asp?type=products&parent=T-REC-x

[25] Viz např. Garfinkel, S.: PGP - Pretty Good Privacy. Šifrování pro každého. Computer Press : Brno, 1998.

Z implementace elektronického podpisu plynou i jeho bezpečnostní záruky. Ty se odvíjejí zejména ze stupně ochrany privátního, jakož i veřejného klíče, nikoliv ze „zašmodrchanosti“ a utajování kryptoalgoritmu. Bezpečnost při používání elektronického podpisu je zejména postavena na tom, že:

1. Nemohlo dojít k narušení tajnosti privátního klíče.
2. Nebyl prolomen použitý kryptoalgoritmus, ani narušena kryptografická bezpečnost hash funkce.
3. 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 v prostředí s velkým počtem uživatelů využíván systém certifikátů poskytovaných nezávislou třetí stranou – certifikační autoritou (poskytovatelem certifikačních služeb).[26]

Mezi hlavní bezpečnostní rizika můžeme považovat:

- odcizení privátního klíče (např. z počítače, přístupného jiným osobám, v případě, že je nedostatečně zabezpečen);
- případ, kdy vydavatel certifikátu si neoprávněně zkopíruje data pro podepisování – soukromý klíč, případně je poskytne neoprávněné osobě;
- narušení jednoznačnosti vazby veřejného klíče na danou osobu, tj. za veřejný klíč dané osoby prezentuje jiná osoba svůj podvržený veřejný klíč;
- rozbití kryptoalgoritmu (lze uvažovat pouze v krajních případech špatně provedeného proprietárního algoritmu, zatímco u prověřených algoritmů používaných standardně pro digitální podepisování je to vyloučeno, resp. pravděpodobnost jejich prolomení při vhodně zvolené délce klíče se blíží k nule).[27]

6.7 AUTENTIZAČNÍ FUNKCE ELEKTRONICKÉHO PODPISU

Můžeme konstatovat, že certifikát je vlastně elektronickým průkazem totožnosti, neboť ten, kdo vytvoří jakoukoliv neprázdnou zprávu a podepíše ji svým soukromým klíčem, může nabídnout protistraně, aby si pomocí certifikátu podepsaného poskytovatelem certifikačních služeb ověřila, že signatář je tou osobou, za níž se vydává (která je uvedena na certifikátu). Tato autentizační funkce je velice vítána jako pomůcka všude tam, kde je na úspěšně provedené identifikaci a autentizaci závislé provedení určité operace (vpuštění do objektu, spuštění počítače, přihlášení do počítačové sítě, autorizace určitého úkonu apod.). V takovém případě se autentizace v rámci organizace zabezpečuje prostřednictvím tzv. *infrastruktury veřejných klíčů.*

Ani elektronické podpisy, ani používání různých přenosových protokolů (např. SSL) však nemohou samy o sobě zajistit dostatečně důvěryhodné prostředí pro elektronickou výměnu dokumentů. Hlavním problémem je totiž práce s klíči – klíčové hospodářství. K tomu je nutný rozsáhlý a komplexní systém, jakým je např. *infrastruktura veřejných klíčů* (Public Key

[26] Kodl, J.: Elektronický podpis. http://www.fzu.cz/texty/ruzne/el_podpis.html

[27] Tento předpoklad je nicméně nepřetržitě testován, neboť skoková změna v technologických možnostech pro prolomení šifry je možná (např. v souvislosti s tzv. kvantovou kryptografií). Takovýto skok je nicméně předvídatelný a rozpoznatelný, takže na něj lze opět reagovat.

Infrastructure, PKI), což lze definovat v širším pojetí jako souhrn hardwaru, softwaru, lidí, metod a procesů potřebných k použití kryptografie veřejných klíčů pro určitou množinu osob.[28]

Jednou z klíčových funkcí poskytovatele certifikačních služeb je svázání identity konkrétní entity (osoby) s konkrétní dvojicí klíčů. PCS musí být subjekt, který se těší všeobecné důvěře (podložené legislativou a rozhodnutím ústředního orgánu – akreditací pro oblast e-governmentu, nebo interními předpisy v rámci podniku či podnikatelské skupiny), a který vydává certifikáty.

Kromě již zmíněných složek bezpečnosti (integrita, autentičnost, nepopiratelnost, důvěrnost) je potřebné mít k dispozici:

1. bezpečnostní zásady definující pravidla, podle kterých musí kryptografické systémy pracovat;

2. systémy pro generování, uchovávání a správu klíčů;

3. předpisy, které by jednoznačně určovaly, jak mohou být klíče generovány, distribuovány a používány;

4. hierarchickou strukturu PCS.

Infrastruktura veřejných klíčů je soubor serverů, poskytovatelů certifikačních služeb (CA), registračních autorit (RA), adresářů a aplikací, které organizacím umožňují elektronicky modelovat důvěru. PKI lze použít pro jednoduché aplikace, např. autentizaci uživatelů a virtuální privátní sítě (Virtual Private Network, VPN), i pro komplexní autorizaci a kontrolu přístupu k aplikacím. PKI slouží ke správě digitálních klíčů a certifikátů, které zajišťují bezpečnost zúčastněných stran. PKI například umožňuje jednotlivci prokázat síti svoji totožnost pomocí certifikátu, prokázat nebo určit vlastnictví dokumentu či přenesené zprávy nebo bezpečně komunikovat s jinou osobou nebo serverem prostřednictvím veřejného komunikačního média, jako je Internet. PKI využívá asymetrické šifrování, veřejné a soukromé klíče, digitální certifikáty a digitální podpisy.

PKI jako produkt neexistuje; je to soubor mnoha spolu integrovaných řešení, které dohromady tvoří infrastrukturu PKI. Dnešní PKI se obvykle skládá z PCS, která vydává certifikáty veřejných klíčů, centrální databáze PKI s odpovídající aplikační logikou a servery, kde jsou k dispozici vystavené certifikáty a seznam certifikátů, kterým byla ukončena platnost. S těmito prostředky pracují programy pro zabezpečení jednotlivých aplikací, jako jsou zejména elektronická pošta, jednotné přihlašování do sítě a aplikací, šifrování a elektronické podepisování souborů, či jiné informační a komunikační služby.

Nejdůležitějším momentem při implementaci PKI je – stejně jako jsme si řekli již dříve u elektronického podpisu – uložení soukromých (tajných) klíčů, které nesmějí být přístupné nikomu jinému než oprávněné osobě. I ze je proto jedním z nejpoužívanějších řešení uložení klíčů na čipovou kartu nebo token.[29]

6.8 LEGISLATIVNĚ-PRÁVNÍ ASPEKTY ELEKTRONICKÉHO PODPISU

Právně má elektronický podpis několik rozměrů a významů, a to podle toho, zda jej chceme užívat v oblasti působnosti soukromého nebo veřejného práva.

---

[28] Jiná definice říká, že PKI (Public Key Infrastructure) – infrastruktura veřejných klíčů, je systém hardware, software, lidí, procesů a politik, který využívá technologii digitálního podpisu pro zajištění průkazného spojení mezi veřejným klíčem a konkrétní entitou.

[29] autentizační předmět, např. přívěšek na klíče obsahující čip a opatřený konektorem USB

6.8.1 Soukromoprávní vztahy s využitím elektronického podpisu

V oblasti soukromého práva, tedy v oblasti, kde mají účastníci rovné postavení, je základním právním institutem právní regulace soukromého práva *smlouva*. Mezi soukromoprávní odvětví se zařazují nejčastěji občanské právo, právo obchodní, právo pracovní, právo rodinné, právo autorské a vynálezecké, mezinárodní právo soukromé a procesní. Právní vztahy související s informačními systémy jsou upravovány zejména právě občanským a obchodním zákoníkem a autorským zákonem.

Nespornost podpisu a jeho uznávání může být v občanskoprávních (a tedy i obchodních) vztazích zajištěna dohodou smluvních stran, a to podle ust. § 2 odst. 3 občanského zákoníku[30] (dále také jen ObčZ): *„Účastníci občanskoprávních vztahů si mohou vzájemná práva a povinnosti upravit dohodou odchylně od zákona, jestliže to zákon výslovně nezakazuje a jestliže z povahy ustanovení zákona nevyplývá, že se od něj nelze odchýlit."* Strany si tedy mohou své vzájemné vztahy upravit tak, jak to odpovídá jejich souhlasné vůli podle svých potřeb.[31] Za splnění podmínky identifikace a autentizace (se současným požadavkem na dodržení principu neodmítnutelnosti, tj. nemožnosti popřít, že podepsaná osoba text skutečně odeslala, případně že příjemce jej skutečně dostal) lze provést elektronickou transakci (například v prostředí Internetu) tak, aby splňovala podmínky ust. § 40, odst. 4 ObčZ, zejména „*... určení osoby, která právní úkon učinila.*"

Používání elektronického podpisu je tedy v soukromoprávních vztazích možné na bázi smluvní volnosti i před nabytím účinnosti zákona o elektronickém podpisu[32] (dále také jen ZoEP) dnem 1.10.2000. Existence zákona vytvořila ovšem podmínky pro zvýšení důvěryhodnosti elektronického podepisování jako takového a umožnila stranám používat instituty, jež byly tímto zákonem poprvé vneseny do našeho právního řádu, jako např. zaručený elektronický podpis, kvalifikovaný certifikát, poskytovatel certifikačních služeb apod.[33]

6.8.2 Veřejnoprávní vztahy s využitím elektronického podpisu

Hlavním principem veřejného práva je poměr nadřízenosti a podřízenosti ve veřejnoprávních vztazích, v jejichž rámci je jedna strana – zpravidla orgán veřejné moci či správy – oprávněna autoritativně rozhodovat o právech a povinnostech strany druhé – fyzické či právnické osoby či skupiny osob. Základním právním nástrojem k výkonu veřejného práva je úřední rozhodnutí. Mezi odvětví veřejného práva se obvykle řadí právo ústavní, právo správní, právo finanční, právo trestní a někdy též občanské právo procesní. V této oblasti fungují informační systémy jako nástroj pro výkon veřejné správy a tedy se na ně vztahuje legislativa, výkon veřejné správy upravující.[34]

---

[30] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

[31] Kromě již citovaného ust. § 40 musí přitom platit zásady formulované v ObčZ (a samozřejmě všechna kogentní ustanovení ObchZ a ObčZ) – např. ust. § 3, odst. 1, § 34 – 37 ObčZ.

[32] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

[33] Více viz rozsáhlá publikační činnost autorova, zejména Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 1. vydání. Praha, C.H.Beck 2001; Smejkal, V. a kol.: Legislativa pro elektronický obchod. Úřad pro veřejné informační systémy, Praha 2001; Smejkal, V.: Elektronický podpis. Pojistné rozpravy, 2001, č. 10, s. 75 – 92; Smejkal,V.: Zákon č. 227/2000 Sb. rok poté. Sborník mezinárodní odborné konferencie „Uľahčí elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti." Bratislava, 20.2.2002, s. 19 – 27

[34] Podle principu uvedeného v čl. 2 odst. 3 Ústavy ČR, podle kterého státní moc slouží všem občanům a lze ji uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.

Používání elektronického podpisu ve veřejné správě proto zůstává stále určitým problémem, a to vzhledem k absenci potřebných konkrétních (pozitivních) právních norem, upravujících výkon veřejné správy s použitím elektronického podpisu, v jednotlivých oblastech. Přetrvávající technologická závislost velkého množství právních předpisů v ČR, vázaných na jediný možný nosič informací – papír – stále brání masovému používání elektronického podpisu v oblasti veřejné správy. I když různé aktivity Ministerstva informatiky se snaží tento stav změnit, největší překážkou je omezený resortní přístup, dále pak neochota ke změnám v zaběhaných, mnohdy až „rakousko-uherských" úředních postupech, izolované aktivity jednotlivých ústředních orgánů a celkově nepřehledný stav českého práva.[35]

Velice stručně můžeme definovat tato hlavní bariéry zavádění elektronického podpisu do veřejné správy:

- První omezení, vyplývající z požadavku § 11 ZoEP,[36] bylo odstraněno 18.3.2002, kdy se prvním akreditovaným poskytovatelem certifikačních služeb stala První certifikační autorita, a.s., dceřinná společnost PVT.
- Druhé omezení, které souviselo s neochotou orgánů veřejné správy zavést možnost používat elektronický podpis tam, kde to zákon již výslovně dovoluje, bylo odstraněno vydáním nařízení vlády, kterým se provádí zákon o elektronickém podpisu, jež vyšlo pod č. 304/2001 Sb. s účinností od 1.10.2001.[37] Toto nařízení uložilo orgánům veřejné moci (tj. orgánům veřejné správy a dalším orgánům státu) zřídit podle povahy a rozsahu své činnosti jedno nebo více pracovišť pro příjem a odesílání datových zpráv (tzv. elektronické podatelny).[38]
- Třetí omezení, vyplývající z již zmíněného čl. 2 odst. 3 Ústavy, je odstraňováno postupně, velice nekoordinovaně, a to nejdříve v rámci samotného ZoEP (novely procesních předpisů, jako občanský soudní řád, správní řád, zákon o správě daní a poplatků a trestní řád), jakož i v rámci zvláštních předpisů.

Abychom ale mohli hovořit o dosažení jednoho z cílů Evropských společenství, tj. plném zrovnoprávnění elektronického podpisu a vlastnoručního podpisu, pak v oblasti veřejné správy, neřku-li e-governmentu, musíme ještě ujít značný kus cesty a vykonat mnoho mravenčí legislativní práce.

6.8.3 Právní ochrana elektronického podpisu a jeho uživatelů

Data pro vytváření a ověřování elektronického podpisu (soukromý a veřejný klíč) jsou chráněna, jako každé jiné údaje na nosiči informací, ustanovením § 257a trestního zákona[39] „Poškození a zneužití záznamu na nosiči informací". Podle dikce tohoto ustanovení kdo získá

---

[35] V oblasti související s aplikací elektronického podpisu viz např. Smejkal, V.: Doručování v českém právním řádu. Justiční praxe. L., 2002, č. 10, s. 572 – 603.

[36] V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. 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.

[37] Smejkal, V., Kodl, J., Mates, P.: Návrh nařízení vlády k provedení zákona o elektronickém podpisu včetně důvodové zprávy. Úřad vlády ČR, Praha 2001.

[38] Podrobnosti viz např. Smejkal, V.: Prováděcí předpisy k zákonu o elektronickém podpisu - část I. IN-SIDE, 2002, č. 4, s. 48 – 51 a část II. INSIDE, 2002, č. 5, s. 44 – 47.

[39] Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů

přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užije,

b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo

c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci, případně vyšší sankcí, pokud spáchá-li tento čin jako člen organizované skupiny, nebo způsobí-li takovým činem značnou škodu či dokonce škodu velkého rozsahu nebo získá-li sobě nebo jinému značný prospěch, resp. prospěch velkého rozsahu.

Podle této skutkové podstaty jsou samozřejmě chráněny před možným útokem pachatele veškeré datové zprávy, obsahující informace, tj. i certifikát nebo jeho část, stejně jako podepsaná zpráva jako celek, nebo její část, tj. elektronický podpis. Podrobný rozbor ustanovení § 257a lze najít v literatuře.[40]

Otázkou zatím soudní praxí neprozkoumanou je, zda soukromý a veřejný klíč jsou osobními údaji chráněnými podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Podle ust. § 4 písm. a) zákona je osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se naopak nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků. Ze soukromého klíče – samotného o sobě – není možno určit subjekt údajů[41] a navíc, vzhledem k nutnosti jej utajovat, není tato situace pravděpodobná. Veřejný klíč je zveřejněn a tedy – prostřednictvím certifikátu – by pravděpodobně osoba, k níž se vztahuje, určená či určitelná byla. Je to poněkud paradoxní. Pak by tento veřejný klíč byl chráněn podle ust. § 178 trestního zákona „Neoprávněné nakládání s osobními údaji“ a jeho neoprávněné sdělení, zpřístupnění, jiné zpracování nebo přisvojení v souvislosti s výkonem veřejné správy nebo v souvislosti s výkonem povolání, zaměstnání nebo funkce je sankcionováno podle zákona odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem, případně - vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká, i více.

Vzhledem k předchozímu je tedy chráněn obdobným způsobem i certifikát, samozřejmě nikoliv proti sdělení či zpřístupnění, neboť to je přímo posláním certifikátu. V tomto případě ale je zajímavá možnost stíhání pachatele v případě, že se pokusí podvrhnout falešný certifikát (např. při útoku typu man-in-the-middle attack, který je důsledkem nedostatečné autentizace na přístupových bodech a u koncových uživatelů), a to nejen podle ust. § 257a, ale i podle klasických skutkových podstat, tradičně definovaných v našem trestním zákonu, jako jsou § 209 – Poškozování cizích práv[42] a v případě majetkového trestného činu § 250 – Podvod. A samozřejmě zde vždy zůstane možnost, v případě že se tak stane např. prostřednictvím Internetu nebo jiného veřejného

---

[40] Zejm. Smejkal, V., Sokol, T., Vlček, M.: Počítačové právo. 1. vydání. Praha, C.H.Beck 1995 a Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 1. vydání. Praha, C. H. Beck 2001.

[41] Viz struktura soukromého klíče popsaná např. v dokumentu PKCS#1 v2.1: RSA Cryptography Standard. RSA Laboratoriem, June 14, 2002, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.doc a PKCS#8: Private-Key Information Syntax Standard. An RSA Laboratories Technical Note, Version 1.2, Revised November 1, 1993, ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-8.doc

[42] Kdo jinému způsobí vážnou újmu na právech tím, že a) uvede někoho v omyl, nebo b) využije něčího omylu, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

telekomunikačního zařízení, zahájení trestního stíhání pro porušování tajemství dopravovaných zpráv podle § 239 a § 240 trestního zákona.

Podepsaný dokument resp. jeho součást, elektronický podpis, by mohly – podle okolností – být rovněž chráněny jako osobní údaje, a to v případě, že by byl ke zprávě připojen certifikát, nebo uvedena adresa jeho uložení (na serveru). I tato otázka by měly být dále teoreticky zkoumána.

Z hlediska ochrany podepisujících osob i příjemců podepsaných zpráv tradičními soukromoprávními prostředky pak je třeba upozornit na obecná ustanovení občanského zákoníku o náhradě škody,[43] na která se odkazuje zákon o elektronickém podpisu v ust. § 5 odst. 2 (odpovědnost podepisující osoby) a § 7 (odpovědnost poskytovatele certifikačních služeb).

6.9 VYUŽITÍ ELEKTRONICKÉHO PODPISU DNES A V BUDOUCNOSTI

Na počátku jsem se zmínil o e-governmentu a e-obchodu, jako dvou základních, modelových případech, kdy potřebujeme dostatečně silné a přitom uživatelsky nenáročné autentizační prostředky. Elektronický podpis takovým prostředkem nepochybně je a pokud budou dořešeny některé spíše legislativní otázky, které se v dalším vývoji ukázaly být aktuální (např. přeshraniční poskytování služeb poskytovatelů certifikačních služeb, časová razítka, bezpečné úložiště podepsaných dokumentů).[44]

Cílovým řešením by mohla být koncepce „elektronického občanského průkazu“, případně „elektronického průkazu zaměstnance“, který by mj. obsahoval i data potřebná pro vytváření elektronického podpisu držitele průkazu, a to jak pro jeho práci (v rámci výkonu zaměstnání nebo funkce při výkonu veřejné správy, tj. v oblasti e-governmentu, tak při jeho působení v rámci jakéhokoliv podnikatelského subjektu provozujícího e-obchod nebo se na něm podílejícího), tak pro užívání tohoto průkazu občanem v pozici účastníka řízení před orgánem veřejné správy (e-government) či jako spotřebitele (e-obchod).

7 KONCEPCE VĚDECKÉ PRÁCE A VÝUKY

7.1 POPIS SOUČASNÉHO STAVU

Jak již bylo uvedeno v úvodu, problematiku bezpečnosti a ochrany dat v ITS chápu jako výrazně mezioborovou disciplínu. Chtěl bych toto opakovaně zdůraznit, neboť výuka a vzdělávání v oblasti bezpečnosti a ochrany dat v ITS je většinou velmi závislá na hlavním zaměření vysoké školy resp. její fakulty a požadavky komplexnosti a systémového přístupu splňuje pouze menšina z dnešních kursů v této oblasti.

[43] Obecná odpovědnost za škodu způsobenou porušením právní povinnosti (§ 420) nebo provozní činností (§ 420a). V souvislosti s elektronickým podpisem je ale zajímavá možnost vzniku odpovědnosti podle § 421a, kdy každý odpovídá i za škodu způsobenou okolnostmi, které mají původ v povaze přístroje nebo jiné věci, jichž bylo při plnění závazku použito.

[44] Viz Smejkal, V. Elektronický podpis v roce 2003. INSIDE, 2003, č. 9, nebo Dumortier, J. a kol.: The legal and market aspekts of electronic signatures. Study Directorate – General Information Society. KU Leuven, Brusel 2003.

Jak vyplývá z průzkumu provedeného v roce 2002,[45] i z vlastních poznatků autorova poměrně rozsáhlého působení v tomto oboru, existují u nás v podstatě tyto hlavní směry výuky (a většinou i vědecké práce) v této oblasti, jak vyplývá z uvedených názvů vyučovaných předmětů:

1. teoreticky zaměřené disciplíny, zaměřené na matematické a informatické základy bezpečnosti, zejména pak kryptologie – např. Kryptografie; Kódování, kryptografie a kryptografické protokoly; Bezpečnost a kryptografie; Kryptografie v informatice; Aplikovaná kryptografie; Utajování datových přenosů; Ochrana dat v informatice; Teorie kódování a šifrování; Kódování a kryptografie atd.;[46]
2. technicky zaměřené disciplíny, pojednávající bezpečnost z určitého, obvykle speciálního hlediska – sem patří zejména předměty jako Bezpečnost a ochrana dat v operačních systémech; Bezpečné systémy (odolnost proti poruchám); Bezpečnostní mechanismy pro počítačové sítě a přenos dat; Správa a bezpečnost operačních systémů; Autentizace a řízení přístupu; Technická ochrana objektů atd.;
3. manažersky zaměřené předměty o bezpečnosti ITS – Bezpečnost informačních technologií (základní znalosti o bezpečnosti ITS, o analýze rizik o tvorbě havarijních plánů, o principech kryptografie, o správě kryptografie, o vybraných bezpečnostních funkcích, o kritériích hodnocení bezpečnosti a o normách bezpečnosti ITS); podobný obsah má předmět Kryptografie a počítačová bezpečnost;
4. jinak zaměřené předměty, obsahující zmínky o bezpečnosti obvykle v rámci jedné přednášky/semestr – Podnikání a obchodování na Internetu (bezpečnost transakcí na Internetu); Komunikační technologie a služby (bezpečnost v sítích); Provozování informačních systémů (bezpečnostní otázky provozu IS/IT – které bezpečnostní otázky garantuje provoz IS a jak je řeší);
5. problematika řízení rizik je většinou orientována na finanční rizika – viz předměty jako Teorie rizika, Řízení finančních rizik; výjimkou jsou obecné předměty Krizové řízení a Základy krizového managementu; samostatným směrem, orientovaným na oblast průmyslové bezpečnosti, nezahrnujícím problematiku bezpečnosti a ochrany dat ITS, je výuka oboru Požární ochrana a průmyslová bezpečnost (VŠB – TUO)
6. právní aspekty jsou až na výjimky přednášeny pouze zcela okrajově, a to v předmětech jako Kriminalistika, Trestní právo hmotné, Autorské právo a průmyslová práva v informační společnosti, Právo duševního vlastnictví apod.; pouze na některých vysokých školách existují předměty jako Informační právo, Počítačové informační systémy (zahrnuje i jednotlivé přednášky na témata Právo na informace a ochrana osobních údajů, Elektronický právní styk, elektronický podpis. Bezpečnost informačních systémů, ochrana hardware, software a dat. Aktuální otázky počítačové a internetové kriminality. Autorskoprávní ochrana počítačových programů a databází, ochrana práv duševního vlastnictví v prostředí internetu.), výjimkou jsou specializované a komplexně pojaté předměty Počítačové a informatické právo resp. Právo informačních systémů a kriminalita na Internetu;

[45] Dočkal, J.: Výuka informační bezpečnosti na vysokých školách. Data Security Management, 2002, č. 4, s. 18 – 20.

[46] Jen na okraj poznamenávám, že někdy jsou předměty vzhledem ke svému obsahu pojmenovány nesprávně; věda o šifrování se nazývá kryptologie a je tvořena kryptografií, coby vědeckou disciplínou aplikované matematiky, zabývající se návrhem šifer, a kryptoanalýzou, která se zabývá procesem opačným, tj. luštěním šifer.

7. zcela výjimečně jsou na některých vysokých školách vyučovány předměty, pojímající problematiku bezpečnosti ITS komplexněji – Ochrana dat a informačního soukromí, Bezpečnost v informačních technologiích, a zřejmě nejuspořádaněji, byť ve velmi omezeném časovém rozsahu, v rámci předmětu Ochrana počítačových dat (Policejní akademie);
8. nehodnotím výuku na Vojenské akademii v Brně, neboť zde je podle názvů předmětů vyučováno mnoho předmětů souvisejících s bezpečností a ochranou dat v IS – např. Prostředky šifrové ochrany informací, Bezpečnostní technologie ochrany informačního systému, Základy kryptologie, Výstavba, údržba a bezpečnost systémů velení, a to vzhledem k nedostupnosti informací o jejich obsahu.

Co se týká odborných akcí v rámci dalšího vzdělávání (vědeckých a odborných seminářů), pak zde existují dva zásadně odlišné směry:

a) teoretické problémy bezpečnosti, obvykle z oblasti kryptologie (viz např. známá Kryptobesídka),
b) praktická, obvykle velmi kasuistická řešení informující o řešení problému obvykle způsobem „*pro řešení problémy XYZ byl v prostředí A použit prostředek B*“; v řadě případů tyto referáty mají větší či menší charakter skrytého public relation (PR).

Jak vyplývá z výše uvedeného přehledu, existují velké rozdíly v zaměření a konkrétním obsahu výuky předmětů, souvisejících s problematikou bezpečnosti a ochrany dat v ITS. Souhrnně bychom mohli konstatovat, že existují tyto základní směry výuky a dalšího vzdělávání:

a) výuka teoretických základů bezpečnosti – obvykle jde o obor kryptologie, případně kryptografie;
b) bezpečnostní projektování – obvykle se zaměřením na analýzu rizik, bezpečnostní politiku, kritéria hodnocení bezpečnosti a normy bezpečnosti ITS;
c) bezpečnostní technologie – obvykle jde o bezpečnostní aspekty operačních systémů, protokoly, řízení přístupu, bezpečnost aplikací, bezpečnost sítí, antivirová ochrana apod.;
d) havarijní plánování a krizové řízení – obvykle univerzální, bez zahrnutí problematiky ITS;
e) právní aspekty bezpečnosti a ochrany dat ITS, případně včetně počítačové kriminality.

Také stávající zaměření vědy a výzkumu se orientuje obdobným způsobem, přičemž do oblasti základního výzkumu spadají především teoretické otázky týkající se kryptografie a přenosu informací. Další otázky jsou záležitostí výzkumu aplikovaného nebo, a to nejčastěji, předmětem inženýrské, byť vysoce kvalifikované činnosti.

7.2 DALŠÍ VÝVOJ VĚDECKOVÝZKUMNÉ ČINNOSTI A VÝUKY V OBORU

Stále roste význam doposud podceňované problematiky řízení a správy bezpečnosti, resp. krizového a havarijního plánování, a to jako ryze manažerského oboru. Druhým „netechnologickým“ a rovněž stále důležitějším oborem je problematika právních aspektů informačních systémů a jejich bezpečnosti. (Není to pouze otázka budování e-governmentu, ale i zkoumání některých aspektů ITS, např. u elektronického podpisu jsou to otázky odpovědnosti, náhrady škody, trestněprávní ochrany elektronického podpisu před zneužitím apod.)[47] Zvýšenou

[47] Viz např. Smejkal, V.: Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, II., 2003, č. 6, s. 161 – 167.

pozornost, opět především z hlediska manažerského a právního, a to včetně tvorby bezpečnostních norem a standardů, lze očekávat z hlediska mezinárodních vztahů a aspektů.

Pokud bychom měli hovořit o zaměření dalšího výzkumu v oboru bezpečnosti ITS a výuky v něm prováděné, je zřejmé, že typ školy (univerzitní/neuniverzitní) a zaměření fakulty (přírodovědní/technické/manažerské/specializované) budou nepochybně ovlivňovat skladbu a obsah předmětů. Dle mého názoru je ale tento vliv ve většině případů příliš silný, možná až zavádějící, neboť tím dochází k absenci komplexního, systémového pojetí bezpečnosti ITS jako takového. Absolventi jednotlivých oborů mají potom v praxi tendenci řešit bezpečnostní problematiku především z hlediska získaných znalostí, tj. zaměřují se na úzce pojaté řešení.[48] Snad největší absenci nacházíme u složky, která je – alespoň dle mého názoru – rozhodující: organizace a řízení bezpečného ITS, tj. management procesu budování, užívání a dalšího rozvoje bezpečného ITS.

Problematika bezpečnostního managementu, která by zahrnovala otázky řízení a správy bezpečnosti organizace a jejího informačního systému, je velkým, multioborovým komplexem předmětů, a mohla by představovat samostatný obor výuky na vysoké škole, především manažerského zaměření. Tím spíše, že bezpečnost a její zajišťování má i svůj rozměr právní a ekonomický (ekonomická efektivnost bezpečnosti ITS, resp. bezpečnost versus náklady na ni).[49] V oblasti bezpečnosti ITS by podle názoru autora bylo možné i daleko větši využití podpůrných nástrojů na bázi umělé inteligence podobně, jako v jiných oborech a aplikacích.[50]

Pokud se jedná o jednotlivé, specializovaně zaměřené předměty, jak jsou výše uvedeny, pak by součástí jejich výkladu mělo být v každém případě konstatování, že neexistují izolované aspekty bezpečnosti, stejně jako neexistují samostatně působící nástroje pro zvyšování bezpečnosti a odstraňování rizik. Dle názoru autora existuje společenský požadavek na vytvoření samostatného tématického oboru „bezpečnostní management“, který by sdružoval všechny výše uvedené aspekty a vychovával odborníky pro řízení a správu bezpečnosti, disponujícími komplexním, mezioborovým vzděláním.

Závěrem bych proto rád uvedl, že komplexní problematika řízení a správy bezpečnosti organizace a jejího informačního a telekomunikačního systému by mohla a měla být začleněna do výuky disciplín v rámci oboru odvětvová ekonomika a management na Fakultě podnikatelské VUT v Brně. Jako účelná se jeví spolupráce s Fakultou informačních technologií VUT, kde je vyučována řada předmětů, majících přímý vztah pro problematice bezpečnosti ITS z hlediska dvou výše uvedených podoborů – teoretického a technologického.

---

[48] Odstrašujícím příkladem mohou být jednorázové kampaně za bezpečnost v různých resortech, podnikatelských skupinách nebo jednotlivých podnicích, kdy se za všeobjímající řešení považuje pořízení určitého hardwarového nebo softwarového prostředku (firewall, antivirový program), aniž by bylo provedeno vyhodnocení rizik a řešeny i bezpečnostní otázky personální, organizační, procesní a jiné.

[49] Ve smyslu již publikovaných úvah vztahujících se k ekonomické efektivnosti ITS obecně; viz např. Molnár, Z.: Moderní metody řízení informačních systémů. 2., rozšířené vydání. Grada, Praha 2001.

[50] Mařík, V., Štěpánková, O., Lažanský, J. a kol.: Umělá inteligence I. - III. Academia, Praha 2000, 1997 a 2001; Smejkal, V. Štědroň, B.: Expertní systém pro volbu a zavádění výpočetní techniky. Sborník mezinárodní konference „Aplikace umělé inteligence AI '87“, Praha, 22.-24.4.1987, s. 148 – 155; Smejkal, V., Rais, K. a kol.: Expertní systém pro volbu prognostických metod. Výzkumný úkol SPEV 908-121-203-SMS03 "Rozvíjení procesu automatizace zejména na bázi dalšího rozvoje a aplikace elektroniky průmyslových robotů a manipulátorů", UVVTŘ 89-3-2-1-12. UVVTŘ, Praha 1989

8 LITERATURA

[1] Dočkal, J.: Výuka informační bezpečnosti na vysokých školách. Data Security Management, 2002, č. 4, s. 18 – 20

[2] Dumortier, J. a kol.: The legal and market aspekts of electronic signatures. European Commission, Directorate – General Information Society. KU Leuven, Brusel 2003

[3] Garfinkel, S.: PGP - Pretty Good Privacy. Šifrování pro každého. Computer Press, Brno 1998

[4] Grant, G.L.: Understanding Digital Signatures. McGraw-Hill, New York 1997

[5] Klíma, V.: Moderní kryptografické metody a standardy. XVIII.konference EurOpen.CZ, 11.6.–13.6.2001. Sborník XVIII.konference EurOpen.CZ, Praha 2001

[6] Klíma, V.: Ochrana dat, verifikace dokumentů a reálné možnosti využití šifrovacích technologií a digitálních podpisů v informační společnosti, Odborná sdělení Kriminalistického ústavu Policie České Republiky, 1999, č. 2, s. 18 – 21

[7] Kodl, J.: Elektronický podpis. http://www.fzu.cz/texty/ruzne/el_podpis.html

[8] Koláček, Š., Sup, J., Smejkal, V.: K základům vědeckého řízeni vyučovacího procesu. Katedra pedagogiky VUT, Brno 1983

[9] Kříž, J., Smejkal, V.: Informatika a daňové systémy. FP VUT v Brně ve spolupráci s Nottingham Business School the Nottingham Trend University, 1.-4 vydání. Brno 1996 - 1999

[10] Mařík, V., Štěpánková, O., Lažanský, J. a kol.: Umělá inteligence I. - III. Academia, Praha 2000, 1997 a 2001

[11] Mates, P.: Ochrana osobních údajů. Karolinum – nakladatelství University Karlovy, Praha 2002

[12] Mates, P., Smejkal, V.: Vedení informačních systémů a zacházení s dokumenty v oblasti zdravotnictví z hlediska elektronického a digitálního zpracování. Výzkumná studie, Ministerstvo zdravotnictví ČR, Praha 1999

[13] Mates, P., Smejkal, V.: Dokumenty budoucnosti, Data Security Management, II., 1998, č. 5, s. 34 a násl.

[14] Mates, P., Smejkal, V.: Elektronické podpisy. Právní rádce, VII., 1999, č.9, s. 17

[15] Menzel, T.: Elektronische Signaturen. Verlag Österreich, Wien, 2000

[16] Molnár, Z.: Moderní metody řízení informačních systémů. 2. rozšířené vydání. Grada, Praha 2001

[17] Musil, J. a kol.: Kriminalistika. Praha, Naše vojsko 1994

[18] Musil, S.: Počítačová kriminalita. Institut pro kriminologii a sociální prevenci, Praha 2000

[19] Rais, K., Smejkal, V. a kol.: Řízení výpočetních středisek na vysokých školách - třetí etapa dílčího úkolu SPEV 90910110, Brno 1985

[20] Smejkal, V.: Hodnocení výkonnosti počítačových systémů. Sborník 12. sympozia Slovenskej kybernetickej spoločnosti pri SAV „Kybernetické aspekty výpočtovej techniky“, Smolenice, 27.-30.1.1986, s. 186 - 192

[21] Smejkal, V. Štědroň, B.: Expertní systém pro volbu a zavádění výpočetní techniky. Sborník mezinárodní konference „Aplikace umělé inteligence AI '87“, Praha, 22.-24.4.1987, s. 148 - 155

[22] Rais, K., Smejkal, V.: Vybrané charakteristiky počítačových systémů a jejich hodnocení Výzkumná zpráva SPEV 909334503/052 „Informační systémy a moderní metody řízení v odvětví kultury a jejich metodologie“. UISK, Praha 1987

[23] Rais, K., Smejkal, V.: Evaluation of Terminal System Performance. Sborník European Congress on Simulation, Praha 21.-25.12.1987, str. 130 - 134

[24] Silverman , R.D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. RSA Laboratories, April 2000 Bulletin #13 (Revised November 2001)

[25] Smejkal, V., Rais, K. a kol.: Návrh expertního systému pro volbu prognostických metod. Výzkumný úkol SPEV 908-121-203-SMS03 „Rozvíjení procesu automatizace zejména na bázi dalšího rozvoje a aplikace elektroniky průmyslových robotů a manipulátorů“ UVVTŘ 88-3-2-1-06. UVVTŘ, Praha 1988

[26] Smejkal, V., Rais, K. a kol.: Expertní systém pro volbu prognostických metod. Výzkumný úkol SPEV 908-121-203-SMS03 „Rozvíjení procesu automatizace zejména na bázi dalšího rozvoje a aplikace elektroniky průmyslových robotů a manipulátorů“, UVVTŘ 89-3-2-1-12. UVVTŘ, Praha 1989

[27] Smejkal, V., Sokol, T., Vlček, M.: Počítačové právo. 1. vydání. Praha, C.H.Beck 1995

[28] Smejkal, V., Mates, P.: Návrh zákona o Úřadu pro ochranu osobních dat včetně důvodové zprávy, Ministerstvo hospodářství ČR, Praha 1995

[29] Smejkal, V., Kunzl., J.: Bank Computer Crime in the Czech Republic. Zvaná přednáška na mezinárodní kongres INSIG „Security in Banking“, Paříž, 27.-30.1.1997

[30] Smejkal, V., Mates, P.: Návrh zákona o ochraně osobních údajů včetně důvodové zprávy. Úřad pro státní informační systém, Praha 1999

[31] Smejkal, V., Mates, P.: Návrh zákona o elektronickém podpisu včetně předkládací a důvodové zprávy a vypořádání připomínkovacího řízení. Poslanecká sněmovna Parlamentu ČR, Praha 1999 – 2000

[32] Smejkal, V., Kodl, J. a kol.: Návrh zákona o informačních systémech veřejné správy. Úřad pro státní informační systém, Praha 2000

[33] Smejkal,V. : Electronic Signature as an Instrument of Development of Electronic Trade in the Law of the Czech Republic. The Fourth International Conference „Small and Medium Management with Computer Support“. September 22, 2000, BMF TU Brno, Czech Republic, pp. 113-118

[34] Smejkal, V.: Outsourcing a jeho smluvní zabezpečení. Proceedings of 8th International Conference „Systems Integration 2000“, Praha, 12.-13. 6. 2000, s. 315 – 322

[35] Smejkal,V. : Electronic Signatures in The Czech Legal System and Their Importance for E - Commerce. University of Trento. Italy. Proceedings of Conference „Transformation of CEEC Economies to EU Standards“, Czech and Slovak Section, November 2000, s. 75-79.

[36] Smejkal, V.: E-Commerce and Legal Relationships on the Internet under the Czech Law. Sborník mezinárodní konference „Electronic commerce and intellectual property rights, protection of domain names, software and databases“, Licensing Executives Society Czech Republic and Licensing Executives Society France, Praha, 2.10.2000

[37] Smejkal, V.: Fungování a vliv elektronického podpisu na e-business a na veřejnou správu. Sborník konference „E-business: strategie a implementace“, Praha 6.-7.3.2001.

[38] Smejkal, V. a kol.: Legislativa pro elektronický obchod. Úřad pro veřejné informační systémy, Praha 2001

[39] Smejkal, V., Kodl, J., Mates, P.: Návrh nařízení vlády k provedení zákona o elektronickém podpisu včetně důvodové zprávy. Úřad vlády ČR, Praha 2001.

[40] Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 1. vydání. Praha, C.H.Beck 2001

[41] Smejkal, V.: Internet a §§§ (Internet a paragrafy). 2. aktualizované, přepracované a doplněné vydání, GRADA, Praha 2001

[42] Smejkal, V.: Open Source, GNU, GPL, patents, copyright and law regulation in the Czech Republic. Konference LinuxBazaar 2001 „LINUX as a subject of business“, Prague, April 24, 2001.

[43] Smejkal, V.: Právní předpoklady pro elektronický obchod v ČR. Proceedings of 9th International Conference „Systems Integration 2001“. Praha, 11.-12.6.2001, s. 47 – 60

[44] Smejkal, V.: Risks involved in the introduction, use and innovation of information technology in small and medium sized firms. Proceedings of Fifth International Conference „Small And Medium Firm Management With Computer Support“, Brno, 21.9.2001, s. 162-170

[45] Smejkal, V.: Trendy ve zvyšování bezpečnosti a odolnost banky v internetovém prostředí. Sborník konference „Bankovní dny IIR“, Institute for International Research, Praha 18.-19.9.2001.

[46] Smejkal, V.: Ochrana osob, organizací a informačních systémů. Právní rádce, 2001, č.10, s. 8 –15

[47] Smejkal,V.: Rechtliche Aspekte des E-Handels im EG und in der Tschechischen Republik. University of Trento. Italy. Proceedings of Conference „Transformation of CEEC Economies to EU Standards“, Czech and Slovak Section, November 2001, s. 163-167

[48] Smejkal, V.: Elektronický podpis. Pojistné rozpravy, 2001, č. 10, s. 75 – 92

[49] Smejkal, V.: Doručování v českém právním řádu. Justiční praxe. L., 2002, č. 10, s. 572 – 603

[50] Smejkal, V.: Prováděcí předpisy k zákonu o elektronickém podpisu - část I. IN-SIDE, 2002, č. 4, s. 48 – 51 a část II. INSIDE, 2002, č. 5, s. 44 – 47

[51] Smejkal,V.: Zákon č. 227/2000 Sb. rok poté. Sborník mezinárodní odborné konferencie „Uľahčí elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti.“ Bratislava, 20.2.2002, s. 19 – 27

[52] Smejkal, V., Bachrachová, H.: Das tschechische Gesetz über die elektronische Signatur. Mezinárodní konference „Internationalen Salzburger Rechtsinformatik Symposions 2002“, Salzburg 20.–24.2.2002. In: Schweighofer, E., Menzel., T., Kreuzbauer, G.: IT in Recht und Staat. Aktuelle Fragen der Rechtsinformatik. Sien, Verlag Österreich 2002, s. 329 – 337

[53] Smejkal, V.: Právní rizika související s CRM. Proceedings of 10th International Conference „Systems Integration 2002“, Praha, 10.-11. 6. 2002, s. 459 – 464.

[54] Smejkal, V.: Lumpáren se nezbavíme. Prognóza dalšího vývoje v oblasti informační a informatické kriminality. (We Will not Get Rid of the Dirty Business. A prognosis of the

future development of information technology crime.) In: Vize informační bezpečnosti 2002 – 2003. Data Security Management, TATE International, s.r.o., Praha 2002, s. 50 – 53

[55] Smejkal, V.: Informatická a počítačová kriminalita. Pojistné rozpravy, 2002, č. 12, s. 142 – 176

[56] Smejkal, V.: Informační systémy veřejné správy v ČR. 1. vydání. VŠE v Praze – Nakladatelství Oeconomica, Praha 2003

[57] Smejkal, V., Rais, K.: Řízení rizik. 1. vydání. GRADA, Praha 2003

[58] Smejkal, V.: Informační systémy veřejné správy v ČR. Analýza současného stavu a návrh na řešení. Ministerstvo informatiky ČR, Praha 2003

[59] Smejkal, V. a kol.: Study on legal and market aspects of the application of Directive 1999/93/EC laying down a Community framework for electronic signatures and on the practical applications of the electronic signature – part: Czech Republic. In: [2]

[60] Smejkal, V.: Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, II., 2003, č. 6, s. 161 – 167.

[61] Smejkal, V. Elektronický podpis v roce 2003. INSIDE, 2003, č. 9, v tisku

[62] Smejkal, V.: Computer Law in the Czech Republic. 1. vydání. Kluwer Law International, 2003, v tisku

[63] Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Citace (CELEX): 399L0093, publikováno v OJ L 013

[64] Svoboda, P., Kroft, M., Beran, K., Emr, D., Frýzek, L., Vána, R., Vít, M.: Právní a daňové aspekty e-obchodu. Linde, Praha 2002

[65] Šámal, P., Púry, F., Sotolář, A., Štenglová, I.: Podnikání a ekonomická kriminalita v České republice. 1. vydání. C.H.Beck, Praha 2001

[66] Vodáček, L., Vodáčková, O. : Management. Teorie a praxe v informační společnosti. 4. rozšířené vydání. Management Press, Praha 2001

9 ABSTRACT

The security of information and telecommunication systems (ICT) is one of the major limitations – and, in the same time, prerequisites – of the e-business and e-government development. Security is not merely technological issue; it has to be treated comprehensively, using the general methods of the management. All the items of security of the information systems have to be warranted, i.e. personal security, administrative security, site security, hardware security, software security, data security and communication security.

On of the most substantial aspects of ICT security is user identification and authentication while ensuring privacy, integrity and undeniability of the message. The traditional approach to the authentication in ICT used to be based on long-term password, which proved to be entirely insufficient. Authentication tokens are quite useful for physical access to ICT. However, they cannot be used for the more and more frequent task of remote access to the systems and data. Therefore, the importance of electronic signature – usually as the digital signature based on the asymmetric cryptography – is growing nowadays. The electronic signature has, however, its managerial and legal aspect in addition to the cryptographic and technological viewpoint.

It is widely accepted that so-called advanced electronic signature fulfills the requirements associated with the traditional personal signature and, moreover, offers additional features that cannot be achieved on the paper; namely, the document integrity protection in the first place. In spite of that, all the governments fail to incorporate the electronic signature quickly into respective national legislations. Conservative approaches of politicians and officials as well as the relative lack of the applications have to be named as the main reasons. There is also management issue: building of public and private PKI´s and ensuring its secure and trustworthy operation.

Similarly, one can say about the directions of research and education on Czech universities that there are a significant number of highly specialized subjects oriented either to the security theory (cryptography) or to the technical practice (protocols, networks, operation systems). The same is true for the business and law training. The security topics are taught as separate subjects out of the mainstream of the law or business education. In author's opinion, there is a social demand for the establishing of the separate, comprehensive and interdisciplinary specialization “security management” integrating all the abovementioned aspects and educating professionals suitable for the management and administration of the security.