Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 9/2002 **15. září 2002**

9/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/

(367 e-mail výtisků)

Obsah : **Str.**

(články neprochází jazykovou korekturou)

A. Deset kroků k e-komunikaci občana se státem!
Mgr. Pavel Vondruška, ÚOOÚ

Tento příspěvek byl připraven pro symposium „Infoforum e-safety aneb bezpečnost dat na internetu“, které se konalo 5.září 2002 na Právnické fakultě Univerzity v Olomouci. Další informace na http://www.infocom.cz/infoforum/olomouc.htm .

Z událostí poslední doby se zdá, že jsme se dočkali – elektronický podpis se začíná používat v některých konkrétních agendách. Sliby voličům o elektronické komunikaci mezi občanem a státem tak dostávají konkrétní podobu. Cesta k této komunikaci nebyla jednoduchá. V tomto krátkém příspěvku připomenu některé kroky, které musely být vykonány, aby vůbec mohla být zahájena.

KROK 1. - ZÁKON

Poté, co před dvěma lety, konkrétně 1.10.2000, vstoupil v účinnost **zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů** (dále jen „zákon č. 227/2000 Sb.“), následovala celá řada dalších, neméně důležitých kroků nutných k tomu, aby mohl být elektronický podpis v komunikaci občan – stát používán.

Zákon č. 227/2000 Sb. uložil **Úřadu pro ochranu osobních údajů** řadu povinností, a proto zde bylo konstituováno příslušné pracoviště – **odbor elektronického podpisu**.

KROK 2. – NAŘÍZENÍ VLÁDY

Dalším důležitým krokem se stalo vydání **nařízení vlády č. 304 ze dne 25. července 2001, kterým se provádí zákon č. 227/2000 Sb**.(dále jen „nařízení vlády č.304“).
Tento právní předpis stanoví povinnost orgánů veřejné moci zřídit **elektronické podatelny** a zajistit jejich provoz, a to v těch případech, kdy ze zvláštních právních předpisů pro tyto orgány vyplývá povinnost přijmout podání učiněná elektronické podobě a elektronicky podepsaná anebo právo činit úkony v elektronické podobě a elektronicky podepsané.
Těmito zvláštními právními předpisy jsou:
- zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů
- zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů
- zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Technické a programové vybavení elektronických podatelen musí vyhovovat **standardu Úřadu pro veřejné informační systémy**.

KROK 3. - VYHLÁŠKA

Na základě zmocnění zákona č. 227/2000 Sb. vydal Úřad pro ochranu osobních údajů vyhlášku č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. Vyhláška se týká především poskytovatelů certifikačních služeb, kteří hodlají vydávat kvalifikované certifikáty, a poskytovatelů, kteří chtějí být pro tuto činnost získat akreditaci. Činnost akreditovaných poskytovatelů je pro komunikaci stát - občan nezbytná, neboť podle § 11 zákona č. 227/2000 Sb. :
„V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané **akreditovanými poskytovateli certifikačních služeb**“.

KROK 4. - AKREDITACE

První akreditaci udělil Úřad pro ochranu osobních údajů v březnu 2002 **První certifikační autoritě a.s**. To znamená, že vznikl subjekt, který prokázal schopnost zajistit vydávání a správu kvalifikovaných certifikátů pro komunikaci občan – stát.

Podmínky pro získání akreditace jsou velmi náročné. Hlavním aspektem je zajištění maximální možné míry bezpečnosti při vydávání a správě vydávaných kvalifikovaných certifikátů. A protože bezpečnost vždy něco stojí, musí uchazeč počítat se vstupními investicemi v desítkách miliónů korun. Náročný je rovněž provoz, a to jak na personální zajištění vysoce specializovanými odborníky, tak i vzhledem k nutnosti nepřetržitého provozu klíčových činností.

I když První certifikační autorita a.s. zůstává prozatím jediným akreditovaným poskytovatelem, další firmy se na akreditaci intenzivně připravují.

Přehled udělených akreditací je zveřejňován ve Věstníku Úřadu pro ochranu osobních údajů a v sekci elektronický podpis na webové stránce http://www.uoou.cz/ .

KROK 5. - NÁSTROJE

Poskytovatelé, kteří vydávají kvalifikované certifikáty, musí používat bezpečný nástroj elektronického podpisu a tato skutečnost musí být ověřena Úřadem pro ochranu osobních údajů. Příslušné ustanovení zákona v § 6, odst.1, písm. j) zní: *„… nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou; toto musí být ověřeno Úřadem pro ochranu osobních údajů*".

Úřad pro ochranu osobních údajů průběžně vyhodnocuje shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu na základě písemné žádosti.

Pokud nástroj elektronického podpisu splnil požadavky stanovené zákonem č. 227/2000 Sb. a Úřad pro ochranu osobních údajů vyslovil shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, je zveřejňován ve Věstníku Úřadu a na jeho webových stránkách (http://www.uoou.cz/ep_nastroje.php3). V současné době obsahuje tento seznam nástroje od čtyř různých výrobců.

Na tento krok se v mediálních vystoupeních popisujících cestu k bezpečné komunikaci státu s občanem většinou zapomíná. Pravdou však je, že kdyby nebyly k dispozici nástroje, které jsou považovány za bezpečné, nemohl by žádný z poskytovatelů vydávat kvalifikované certifikáty (přesněji: nemohl by je důvěryhodně podepsat) a nemohl by zveřejňovat seznamy kvalifikovaných certifikátů, které byly zneplatněny (opět z důvodu, že by takový seznam nemohl důvěryhodným způsobem podepsat).

KROK 6. - ZÁKON č.226/2002 Sb.

Šestým krokem můžeme nazvat zákon č. 226/2002 Sb. ze dne 9.5.2002.

Novela se týká zákona č. 227/2000 Sb., o elektronickém podpisu a dále správního řádu (zákon č. 71/1967 Sb), občanského soudního řádu (zákon č. 99/1963 Sb), zákona o správě daní a poplatků (zákon č. 337/1992 Sb.), a trestního řádu (zákon č. 141/1961 Sb.).

Novela zákona o elektronickém podpisu, kterou tento zákon provádí, upravuje pouze § 11. Jak jsem již v části 3 uvedl, tento důležitý paragraf před úpravou zněl:

“V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.“

Tímto zákonem byly na konec odstavce doplněny tyto věty: „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.“.

Důsledkem této poslední novely zákona o elektronickém podpisu tedy je, že pro komunikaci s orgánem veřejné moci nelze používat „anonymní“ certifikát. Z položek v certifikátu musí subjekt, se kterým orgán veřejné moci komunikuje (tedy ne každý subjekt!), být schopen jednoznačně určit držitele kvalifikovaného certifikátu.

Modelovým příkladem takovéto komunikace je např. komunikace s Ministerstvem práce a sociálních věcí (MPSV), které zahájilo projekt podávání žádostí o dávky sociální podpory elektronickou cestou. Jako součást kvalifikovaného certifikátu vyžaduje MPSV (v souladu s touto novelou) identifikátor klienta MPSV. Tento identifikátor si musí nechat podepisující se osoba zapsat do svého kvalifikovaného certifikátu při jeho vystavení.

V dalším výkladu se omezím již jen na změnu správního řádu, jelikož ta se dotýká velkého počtu komunikujících subjektů.

Správním orgánům se zde nově ukládá povinnost zveřejnit na své úřední desce nebo způsobem umožňujícím dálkový přístup (např. na internetovém serveru orgánu) následující informace:

- úřední hodiny, ve kterých je otevřena podatelna,
- elektronickou adresu své podatelny,
- formu technického nosiče pro doručování podání v elektronické podobě,
- seznam kvalifikovaných certifikátů zaměstnanců nebo elektronické adresy, na nichž se nacházejí,
- další možnosti učinit podání pomocí jiných elektronických přenosových technik.

Zákon č. 226/2002 Sb. nabyl účinnosti dne 1. července 2002. To znamená, že od tohoto data mohou občané uvedené informace vyžadovat a správní orgány budou mít povinnost je zveřejnit. Jelikož se dané údaje týkají elektronických podatelen, je nutné při jejich zřizování a konfiguraci vycházet ze standardu ISVS č. 16/01.01, který stanoví požadavky na technické a programové vybavení podatelen.

KROK 7. - STANDARD ÚVIS

Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu (016/01.01) byl uveřejněn ve Věstníku ÚVIS, ročník III, částka 1, 2002. Tento standard byl schválen 30.4.2002 a vyhlášen 25.6.2002, od kdy je také účinný.

Standard se zabývá provozem a atestací elektronických podatelen. Elektronická podatelna je podle tohoto standardu informačním systémem veřejné správy. Pro prokázání shody elektronické podatelny s tímto standardem se ovšem nevyžaduje atest elektronické podatelny. Ten je vyžadován pouze na technické vybavení podatelny a související dokumentaci. Technické vybavení elektronické podatelny musí splňovat požadavky článku 4.5 Standardu ISVS č. 016/01.01. Jedná se především o požadavky na funkčnost - ukládání přijatých zpráv, ověřování elektronických podpisů, formáty a kódování zpráv apod. Standard doporučuje, aby atest byl prováděn i s ohledem na bezpečnost, bezporuchovost a použitelnost vybavení.

Orgán veřejné moci může při akvizici elektronické podatelny postupovat v zásadě dvěma způsoby. Je možné pořídit vybavení, které již úspěšně prošlo atestačním řízením, nebo zažádat a projít procesem atestace na vlastní náklady. V obou případech bude ovšem nutné vlastními silami zpracovat bezpečnostní projekt elektronické podatelny a Evidenční listy pro akvizici vybavení a jeho uvedení do provozu (tyto listy se poté zasílají na ÚVIS).

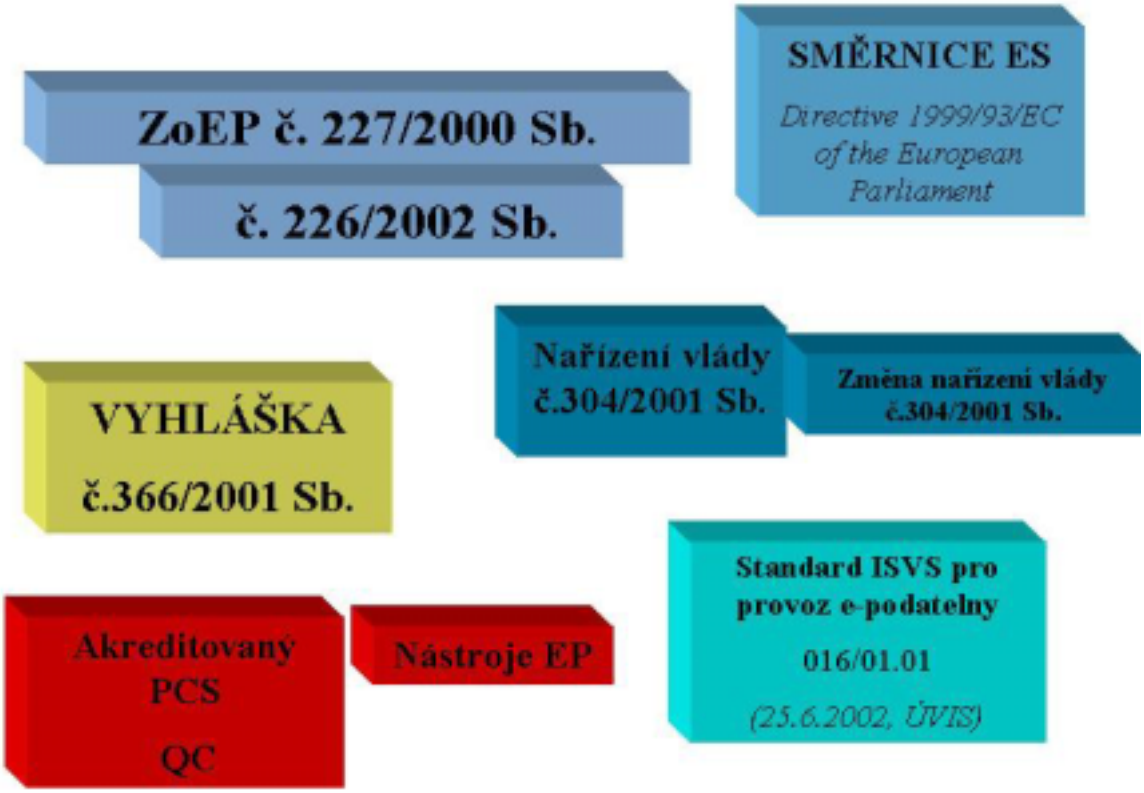
K tomuto standardu existují odborné a věcné připomínky, které se týkají jednak doprovodných komentářů, jednak znění některých odstavců a je pravděpodobné, že bude nahrazen v dohledné době upraveným standardem.

KROK 8. – AGENDY

Na konferenci Internet ve státní správě a samosprávě (ISSS) 25.-26.března v Hradci Králové byly takové dvě připravované agendy představeny. Ředitel odboru informatiky MPSV (Ministerstvo práce a sociálních věcí) ing. Kučera představil možnost elektronického podání žádosti o dávky státní sociální podpory. Přípravu této agendy umožnila novela zákona č.271/2001 Sb., ze dne 10.6.2001, kterou se změnil zákon č. 117/1995 Sb., o státní sociální podpoře. V této novele je uvedeno, že *„ ...podání nebo jiný úkon lze učinit ... i v elektronické podobě a elektronicky podepsat podle zvláštního právního předpisu* (tj. zákona o elektronickém podpisu č.227/2000 Sb.), *pokud MPSV příslušný tiskopis v elektronické podobě zveřejnilo“*.

Tato agenda je již v současné době zpřístupněna a stala se tak jakýmsi modelovým příkladem pro podobné agendy.

Elektronické formuláře žádostí o jednotlivé dávky státní sociální podpory (SSP) a formulář hlášení změn v tomto systému zveřejnilo MPSV na své adrese http://www.mpsv.cz/ . Žádosti je možné podat podepsané pomocí zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, který vydal akreditovaný poskytovatel certifikačních služeb. Jako součást kvalifikovaného certifikátu vyžaduje MPSV (v souladu s novelou zákona č.227/2000 Sb.) identifikátor klienta MPSV. Tento si musí nechat podepisující se osoba zapsat do svého kvalifikovaného certifikátu při jeho vystavení.



Ing. Michal Faltýnek, ředitel odboru Automatizace daňové soustavy a informačních technologií Ministerstva financí potvrdil na stejné konferenci ISSS, že daňová správa na

řešení podávání různých typů daňových přiznání pomocí on-line komunikace přímo přes internet pracuje. Projekt bude uváděn do praxe po jednotlivých etapách. Plné využívání celého projektu odhadl do dvou let.

Z těchto příkladů je zřejmé, že v případě využití elektronického podpisu v nějaké agendě je vždy nejprve nutné provést důkladnou analýzu příslušných právních předpisů a zjistit, zda není nutné provést jejich novelu. Může se totiž stát, že ve stávajících předpisech se striktně vyžaduje např. písemná podoba některého formuláře nebo přílohy. Toto musí vyřešit vhodná úprava těchto právních předpisů, která umožní plné využití elektronického podpisu ve smyslu zákona o elektronickém podpisu č.227/2000 Sb. i v těchto agendách.

Podívejme se na krátký výběr právních předpisů, které umožňují použití elektronického podpisu.

I. Na výrobce zboží, kteří uvádějí na trh výrobky v obalech, a firmy, které obaly vykupují, se vztahuje vyhláška č.117/2002 Sb. Ministerstva životního prostředí ze dne 16. března 2002 o rozsahu a způsobu vedení evidence obalů a ohlašování údajů z této evidence. Ta umožňuje výkazy za uplynulý kalendářní měsíc zasílat ministerstvu v elektronické podobě podepsané podle zvláštního právního předpisu.

II. Zákon o podpoře výzkumu a vývoje č. 130/2002 Sb. umožňuje poskytovateli stanovit způsob podání návrhů a předložení projektů elektronicky, podepsaných podle zákona o elektronickém podpisu.

III. Třetím příkladem je vyhláška č.178/2002 Ministerstva financí ze dne 19. dubna 2002 o podrobnějších pravidlech pro plnění povinnosti oznámit podíl na hlasovacích právech.
Osoba, které vznikla oznamovací povinnost, odešle oznámení o dosažení, překročení nebo snížení podílu na hlasovacích právech Komisi pro cenné papíry, Středisku cenných papírů a společnosti elektronickou poštou a opatří je zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

IV. Obdobný je další příklad využití elektronického podpisu. Jedná se o hlášení obchodů s investičními instrumenty uzavřených mimo veřejný trh (vyhláška č. 105/2001 Ministerstva financí ze dne 9. března 2001).
Povinná osoba může zaslat příslušné hlášení elektronicky, a pokud je opatří zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb, má se tato povinnost za splněnou a nemusí toto hlášení zasílat dodatečně v tištěné podobě opatřené podpisem nebo předat elektronicky na nosném médiu.

V. Známé je také využití elektronického podpisu ve zdravotnictví. Použití podpisu se řídí zákonem č. 260/2001 Sb. ze dne 26. června 2001, kterým se mění zákon č. 20/1966 Sb., o péči o zdraví lidu. V Čl.I, páté části (zpracování osobních údajů souvisejících se zajišťováním zdravotní péče) se stanoví pro zápis zdravotnické dokumentace, aby se v případě, že byl zhotoven na paměťovém médiu výpočetní techniky a neobsahuje zaručený elektronický podpis, dodatečně převedl na papírový nosič (tiskovou sestavu), aby byl dále opatřen datem a podpisem osoby, která zápis provedla, a zařazen do zdravotnické dokumentace pacienta. Pokud se vede zdravotnická dokumentace pouze na paměťových médiích výpočetní techniky, lze zápis zdravotnické dokumentace provádět jen za podmínky, že všechny samostatné části

zdravotnické dokumentace obsahují zaručený elektronický podpis osoby, která zápis provedla, podle zvláštního právního předpisu (zákon č.227/2000 Sb.)

Předpokládá se, že počet zákonů, vyhlášek a směrnic, které upravují konkrétní využití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, se bude dále postupně zvyšovat a budou tak postupně otevřeny další konkrétní agendy, kde lze komunikaci s využitím elektronického podpisu podle zákona č.227/2000 Sb. využít.

KROK 9. – Ministerstvo informatiky

O tom, že vláda přikládá této rychle se rozvíjející oblasti velký význam, svědčí zahájení legislativního procesu, který umožní zřízení Ministerstva pro informatiku. Vzhledem k tomu, že se dá předpokládat, že toto ministerstvo bude mít i kompetenci k elektronickému podpisu a elektronické komunikaci vůbec, může sehrát významnou roli v koordinaci procesu využívání elektronického podpisu při komunikaci občanů se státní správou, resp. v procesu otevírání různých agend, ve kterých lze elektronickou komunikaci uplatnit.

KROK 10. – ZÁVĚR

Předpovídat dynamiku vývoje v této oblasti je velmi obtížné, závisí na mnoha různorodých faktorech. Jmenujme alespoň vývoj v Evropském společenství, rychlost legislativních úprav stávajících zákonů, velikost nutných investic, odborný přístup, prosazení správných myšlenek, nadšení jednotlivců, kteří mohou ovlivnit vývoj v určité oblasti, schválení vhodných norem a standardů, konkurence mezi poskytovateli certifikačních služeb, nabídka levných a bezpečných čipových karet apod.

Elektronický podpis si svoje místo v našem životě najde, stejně jako si ho našly počítače, mobilní telefony nebo Internet. Nebuďme při jeho pomalém zavádění netrpěliví. Často se kriticky uvádí, že od přijetí zákona o elektronickém podpisu uplynuly už dva roky, ale my bychom zde chtěli spíš říci, že uplynuly teprve dva roky. Tato doba posloužila k tomu, aby byly dokončeny některé legislativní práce, vznikly první projekty ve státní správě, byla udělena první akreditace poskytovateli certifikačních služeb, vyhodnoceny první nástroje pro poskytovatele. A především tyto dva roky posloužily k tomu, abychom se dozvěděli, že cosi takového jako je elektronický podpis existuje a k čemu nám může sloužit.

Na závěr uvádím citaci z informačního letáku Úřadu pro veřejné informační systémy – „Komunikační infrastruktura – předpoklad budování informační společnosti“ :
„Obyvatelé získají přímý a bezpečný přístup k veřejným informacím prostřednictvím Internetu. Nejméně 10% kontaktů veřejné správy bude na konci roku 2002 realizováno elektronicky.

Literatura

[1] Bosáková,D., Kučerová,A., Peca,J., Vondruška,P. : "Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů", Nakladatelství ANAG, 2002, 140 stran
http://www.anag.cz/shop/index.php?page=product&id=21&pid=3370

[2] Vondruška, P., Bosáková, D.: "Poskytovatelé certifikačních služeb v EU a ČR, část II.", Data Security Management, DSM 5/2001, str. 36-39, Praha

[3] Vondruška, P.: "E-komunikace začíná !" , Veřejná správa 41/2001, str.12-13, Praha 2001

[4] Vondruška, P: "Elektronický podpis" , 41 stran, Informace a komunikace, Řízení místních orgánů, březen 2002 , RAABE

[5] Vondruška, P.: "Elektronický podpis, Část III. - Legislativa v České republice" , 26.12.2001, EBIZ, http://www.ebiz.cz/article.phtml?cha_id=136&art_id=3455

[6] Vondruška, P.: E-komunikace, e-platby, e-projekty, e-platformy a „velcí hráči“ , Crypto-World 4/2001, http://www.mujweb.cz/veda/gcucmp

[7] Hobza, J.: Elektronické podatelny č. 2, seriál článků o elektronickém podpisu, Veřejná správa 2002, v tisku, http://www.volny.cz/honzahobza/

[8] Hobza, J.: Nové povinnosti správních orgánů, seriál článků o elektronickém podpisu, Veřejná správa 26/2002, http://www.volny.cz/honzahobza/

[9] Sborník konference ISSS, Hradec Králové , 2002

[10] Komunikační infrastruktura – předpoklad budování informační společnosti, informační leták ÚVIS, 2002

[11] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://www.ict.etsi.org/EESSI/Documents/e-sign-directive.pdf

[12] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb., http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

[13] Zákon č.226/2002 Sb. ze dne 9.5.2002, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, a zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) ,
http://www.mvcr.cz/sbirka/2002/sb087-02.pdf

[14] Vyhláška ÚOOÚ 366/2001 Sb. (k Zákonu o elektronickém podpisu č.227/2000 Sb.)
(Vyhláška Úřadu pro ochranu osobních údajů ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu), http://www.mvcr.cz/sbirka/2001/sb138-01.pdf

[15] Nařízení vlády č.304/2001 ze dne 25. července 2001
(Nařízení vlády č.304 ze dne 25. července 2001, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)), http://www.mvcr.cz/sbirka/2001/sb117-01.pdf

[16] Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu, 016/01.01 , http://www.uvis.cz

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 6. Protokol OCSP (Online Certificate Status Protocol).

Jaroslav Pinkava, AEC spol. s r.o.

1. Úvod

Klasickou cestou k ověřování platnosti digitálního certifikátu je obrácení se na aktuální seznam odvolaných certifikátů CRL. Vzhledem k tomu, že CRL bývá vydáváno pouze v určitých časových intervalech (např. jedenkrát denně) je v některých situacích (např. při převodu velké finanční částky či při uskutečňování větších obchodů) žádoucí mít přístup k aktuální informaci o statutu digitálního certifikátu. Za tímto účelem byl vytvořen protokol, který umožňuje zjišťovat aktuální stav (platnost) digitálního certifikátu bez nutnosti užití CRL.

2. Základní vlastnosti protokolu OCSP

Protokol OCSP umožňuje navazujícím aplikacím stanovit revokační statut určitého certifikátu. Klient protokolu OCSP dává požadavek (vzhledem k statutu certifikátu) vůči odpovídající straně (OCSP responder) a pozdrží akceptaci certifikátu do té doby než dostane odpověď na svůj požadavek. Samotný protokol specifikuje obsah a formát dat, která budou vyměněna mezi aplikací, která ověřuje statut certifikátu a serverem, který poskytuje tento statut.

Požadavek OCSP obsahuje následující data:
- verze protokolu;
- požadavek na službu;
- identifikátor příslušného certifikátu;
- nepovinná rozšíření, která může zpracovávat server OCSP.

Po přijetí požadavku server OCSP určí zda:
- zpráva je správně koncipována;
- odpovídající strana je nakonfigurována tak, že může poskytnout požadovanou službu;
- požadavek obsahuje informace, které odpovídající strana potřebuje.

Pokud není některá z těchto podmínek splněna, je odpovědí chybová zpráva. V opačném případě je zpracovávána požadovaná odpověď. Odpovědi OCSP mohou být různých typů. Obsahují tedy typ odpovědi a bajty, ve kterých je obsažena aktuální odpověď. Přitom existuje jeden základní typ odpovědí, který musí být podporován všemi OCSP servery a klienty.

Všechny zprávy obsahující odpověď musí být digitálně podepsány. Příslušný klíč musí patřit někomu z následně vyjmenovaných:
- CA, která vydala příslušný certifikát;
- Důvěryhodná odpovídající strana (Trusted Responder), jejímuž veřejnému klíči důvěřuje klient, který vznesl požadavek;

- Odpovídající strana, kterou k tomu delegovala CA (Authorized Responder), tato strana je vlastníkem speciálně označeného certifikátu, který vydala CA. V tomto certifikátu je specifikováno, že odpovídající strana je oprávněna vydávat OCSP odpovědi v zastoupení této CA.

Zpráva (odpověď) obsahuje:
- číslo verze pro syntaxi odpovědi;
- jméno odpovídající strany;
- odpověď ve vztahu ke každému certifikátu obsaženému v požadavku;
- nepovinná rozšíření;
- OID podpisového algoritmu
- podpis spočítaný nad hashí odpovědi.

Odpověď ve vztahu ke každému z certifikátů (z požadavku) sestává z:
- identifikátor cílového certifikátu;
- hodnota statutu certifikátu;
- interval, po který platí zaslaná odpověď;
- nepovinná rozšíření.

V rámci specifikace v daném materiálu (lit. [2]) jsou definovány následující indikátory hodnoty statutu certifikátu:
- platný (good);
- odvolaný (revoked);
- neznámý (unknown).

Je třeba si uvědomit, že kladná (good) odpověď znamená pouze to, že dotyčný certifikát nebyl odvolán, ale vůbec již není potvrzením toho, že dotyčný certifikát byl někdy vydán či toho, že období jeho platnosti zahrnuje časový okamžik, ve kterém je zasílána tato odpověď. Rozšíření v odpovědi mohou dle dohody obsahovat další informace ohledně statutu certifikátu (např. právě kladné potvrzení toho, že certifikát byl vydán, že platí atd.).

V případě, že nastane nějaká chyba, zasílá odpovídající strana chybovou zprávu (nepodepsanou). Chyby mohou být následujících typů:
- malformedRequest
- internalError
- tryLater
- sigRequired
- unauthorized

3. Funkční požadavky

Pro podporu protokolu OCSP, tj. zajištění přístupu pro klienty OCSP by certifikační autorita měla vytvořit v certifikátech rozšíření AuthorityInfoAccess (dle lit. [3]). Zároveň by mělo být na OCSP klientu nakonfigurováno umístění OCSP odpovídající strany (accessLocation).

Klienti OCSP po obdržení podepsané odpovědi mají ověřit, že:
- certifikát v odpovědí je týž jako v žádosti;
- podpis na odpovědi je platný;

- totožnost podepsané strany je táž jako v zamýšleném příjemci požadavku;
- podepsaná stran je oprávněna podepisovat tyto odpovědi;
- čas odpovědi je dostatečně aktuální;
- zda časový moment, ve kterém bude dostupná nová informace o statutu certifikátu (nextUpdate) je větší než aktuální čas.

4. Další poznámky

Dokument rfc.2560 obsahuje dále v kapitole 4. popis ASN.1 syntaxe protokolu OCSP (žádost o ověření certifikátu pomocí OCSP a odpověď na tuto žádost). Opírá se přitom o pojmy zavedené již v rfc.2459 (lit. [3]). Je zde také uvedena řada technických doporučení pro realizaci OCSP protokolu. Jedná se např. o práci s časovými intervaly, označení oprávněných odpovídajících stran a jejich podpisových klíčů, povinné a nepovinné kryptografické algoritmy, využití tzv. nonce (nikdy se neopakující se hodnota), odkazy na CRL, typy akceptovatelných odpovědí atd.

V kapitole 5. jsou obsaženy některé poznámky k bezpečnostním aspektům služby OCSP. Aby služba OCSP byla efektivní, musí mít klient OCSP možnost vytvořit aktuální spojení se serverem poskytujícím OCSP odpovědi. V případě, že spojení nelze uskutečnit, musí fungovat jako záloha možnost obrátit se k využití CRL.

Za zápor popsané služby lze považovat existenci útoků, které spočívají v zahlcení některé ze stran OCSP protokolu zasíláním falešných zpráv. Tím může být např. velké množství žádostí o potvrzení statutu certifikátů v rámci OCSP služby nebo naopak zasílání (falešných) nepodepsaných chybových hlášení žádající straně. Pokud jsou používány předem spočtené odpovědi (z důvodů urychlení práce serveru), pak existuje rovněž nebezpečí znovuzaslání těchto odpovědí (replay attack) - před ukončením doby platnosti certifikátu, ale již po jeho odvolání.

V příloze A. je popsáno použití protokolu OCSP (příslušné formáty) v rámci HTTP. Příloha B. pak obsahuje detailní syntaxi protokolu OCSP.

5. Literatura

[1] PKIX Working Group: http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

[2] RFC 2560-Online Certificate Status Protocol - OCSP: http://www.ietf.cnri.reston.va.us/rfc/rfc2560.txt

[3] RFC 2459: http://www.ietf.cnri.reston.va.us/rfc/rfc2459.txt

C. Elektronický podpis - projekty v Evropské Unii. Část II.

Jaroslav Pinkava, AEC spol. s r.o.

5. Shrnutí

Kombinované použití čipových karet a technologie PKI spolu se složitostí operací, které provádí certifikační autority má podstatný vliv na cíle a organizaci PKI projektů. Například - postupy pro manažování práce s kartami musí být v souladu s postupy pro manažování práce s certifikáty.

Také je třeba dbát na informovanost uživatelů a jejich zkušenosti při práci s čipovými kartami a chápání (akceptaci) jednotlivých aplikací, které umožňují návaznost na PKI. Kombinace čipové karty, čtečky a softwaru ovlivňuje dynamiku vlastních realizací (je zde více technických problémů, je třeba širší technická podpora). Přítulnost ("user friendly") vlastních aktivit by měla dosáhnout takové úrovně, že činnost PKI je neviditelná pro koncové uživatele (ti nepotřebují znát konkrétní technologii). Toto samozřejmě závisí na připravenosti řešení.

Současné investiční modely jsou většinou poměrně složité a je obtížné provést odhad návratnosti investic. Dle zpracovatelů studie by se měla zlepšit v tomto směru zejména úvěrová činnost.

Větší část projektů se potýkala s technickými problémy ve vztahu k implementacím na čipových kartách. Často to mělo význačný dopad na postup celého projektu (instalace čteček, driverů a aplikačního softwaru, uložení klíče na kartě).

Problematika rozkrytí klíče (key recovery) není v studii analyzována vzhledem k nedostatku odpovídajících norem (což zpětně činí problémy v implementacích). Např. také dokumenty ETSI odmítají pro podpis "key recovery" z principu.

Samotné PKI není v současné době obecně interoperabilní vzhledem k obrovskému množství existujících systémů, platforem, specifikací a požadavků (karty, čtečky, middleware, aplikace).

Legislativa (národní, evropská) je široce přijímána v téměř všech projektech. Některé projekty musely posunout svůj obsah vzhledem k vzniklým zákonům. Již obecně je však rozpoznávána potřeba zajistit shodu s legislativními požadavky.

Naopak vznikají doporučení pro jasné definice v zákonech a normách, tak aby praxe mohla potom jasně vyhodnotit vzniklou shodu s těmito požadavky. Často je konstatováno, že v současnosti neexistují vhodné normy (ekvivalentně viz ČR) či lepší politiky, tak, aby formální požadavky legislativy mohly být uskutečněny v praxi. Je také zatím velmi omezená nabídka pojištění v návaznosti na vydávaní certifikátů.

Studie zde dále konstatuje, že práce v oblasti norem pro elektronický podpis zatím nedosáhly požadovaného stadia a také nejsou v celé řadě projektů adekvátně implementovány.

6. Doporučení

A. Investiční a organizační aspekty:

Materiál konstatuje, že využití čipových karet má podstatný vliv na organizaci PKI projektů. Hlavními důvody pro toto tvrzení jsou:

Řízení práce s kartami musí probíhat souběžně s řízením práce s certifikáty.

- Výroba: grafický čip (techniky tisku);
- Vydání karty (generování klíče, personalizace, dodávka);
- Obnova (update) informací (certifikátů, informací o uživateli);
- Fáze používání;
- Obnova karty.

Informovanost a proškolenost koncových uživatelů je nezbytná pro podporu využívání a akceptace čipových karet v rámci PKI a návazných aplikací.

Aplikace koncového uživatele musí spolu s čipovou kartou pracovat prostřednictvím vhodného softwaru a čtečky. Koncový uživatel žádá přítulné ("user friendly") řešení.

Kombinace hardwaru a softwaru má vliv na stav realizace projektu - je třeba řešit více technických problémů, větší zkušenosti personálu atd.).

Investiční model je komplikovaný a návratnost investic zatím nebyla dosažena v žádném z projektů (analyzovaných v materiálu).

Projekty, které vydávají své vlastní čipové karty, spolupracují s dodavateli softwaru a integrátory za účelem dosažení přítulného ("user friendly") řešení.

Obecně je konstatováno, že by měla být lépe definována a ověřována role a "viditelnost" organizací, které dodávají či vyžadují PKI řešení, která pracují s čipovými kartami. Lépe propracované investiční plány v této oblasti mohou napomoci dalšímu rozšíření daných technologií. Přítulnost řešení by měla dosáhnout úrovně, kdy konkrétní uživatelé nemusí přemýšlet o vlastních použitých technologiích.

Doporučení.

1. Silně podpořit nejlepší organizační postupy (využít k tomu analýzu existujících projektů v Evropě i mimo ní - USA, Asie).

2. Definovat globální metodologii pro výstavbu projektů pro PKI a čipové karty (SCPKI) včetně organizačních, technických a legislativních aspektů.

3. Definovat příručky pro procesy - registrační, personalizační a dodavatelské - pro velkoobjemová SCPKI řešení.

4. Analyzovat funkční investiční modely obsahující:

- referenční náklady;
- možné zdroje financování;

- rozpoznání a analýza vstupu SCPKI do obecných obchodních požadavků.

5. Lépe prozkoumat situace, kdy zvnějšku získaný model PKI je uvnitř (organizace) přetvářen na SCPKI.

6. Analyzovat nejlepší cesty pro odvolávání (revokace) certifikátů, karet.

7. Navrhnou implementační příručku pro návazné služby (bezpečná archivace, validace, časové značky,…). Často zde chybí referenční implementace.

B. Technické aspekty:

V materiálu je konstatováno, že velká řada projektů se potýkala s technickými problémy vzhledem k aplikacím v návaznosti na čipové karty. Podstatně to pozdrželo implementace projektů. Zejména se to týká:

Implementace karet:
- instalace čteček je časově náročnou záležitostí a tudíž je drahá;
- drivery a aplikační software neposkytují vždy dostatečnou přítulnost ("user friendly");
- uložení kořenového (z hlediska uživatele) klíče na kartě je stále diskutabilní;

Politika rozkrytí klíče:
- neexistují jasné normativní postupy pro odpovídající řešení rozkrytí klíče a zálohovací mechanismus při bezpečných řídících procedurách.

Poznámka (J. Pinkava): Vzhledem k známým problémům s definováním postupů pro key recovery v Anglii (odpovídající návrh byl rozbit) je známa nechuť odborníků připravit nový návrh v tomto směru. Vyskytují se dokonce názory, že něco takového je v principu nemožné.

Podepisovací software:
- v době přípravy studie nebyly zjištěny žádné aktuální a zřejmé trendy nebo neobjevilo se řešení, které je zjevným leaderem na trhu.
- Některé projekty mají svoji vlastní politiku pro schvalování řešení podepisovacího softwaru, který je použit v aplikacích.

V analyzovaných projektech byla technická rozhodnutí prováděna velice různými cestami. Toto může vyústit v malou interoperabilitu jednotlivých SCPKI projektů a návazných aplikací a již toto samo může brzdit další rozvoj takovýchto aplikací.

V dalším by měly být analyzovány následující aspekty:

1. Vývoj referenční platformy pro testování integrace systému a jeho interoperability.

2. Zdůraznit význam interoperability jako klíčového faktoru pro úspěšnost řešení a přijmout kroky k její podpoře.

3. Orientovat se na specifické aspekty interoperability jako jsou čipové karty, digitální certifikáty, interakce a vzájemné rozpoznání různých systémů, platforem, specifikací a požadavků pro karty, čtečky, middleware a aplikace.

Doporučení.

1. Podporovat materiály a doporučení EESSI pro SCPKI. Je třeba prezentovat a šířit jejich podstatu a úlohu. Platí to také ve vztahu k materiálům CEN/ISSS a ETSI.

2. Definovat a šířit vysokoúrovňové normy pro software elektronického podepisování. Vytvořit seznam dodavatelů, jejichž produkty jsou vyhodnoceny ve shodě s normami a to i v součinnosti s místní administrativou.

3. Vzít do úvahy, že nedostatek dostupných a spolehlivých produktů často vede k zpoždění v termínech projektů.

4. Ověřit a identifikovat balíky produktů, které jsou v souladu s normami EESSI (v současné době jsou na trhu málo dostupné). Zajistit harmonizaci a legislativní interoperabilitu mezi různými akreditačními schématy v členských zemích platících v současnosti.

5. Uzřejmit si dopad architektury PKI (počet CA, subCA, křížově certifikované CA, bridge CA,…).

6. Zanalyzovat dopad rozlišností národních a evropských norem.

7. Definovat interoperabilní požadavky použitím funkcionální a investiční analýzy projektů. Zřejmé je, že národní projekty pro identifikační karty prakticky stanovují základní pravidla a ostatní projekty se jim přizpůsobují.

8. Podporovat takové práce, které ve svých důsledcích vedou ke koherenci národních akreditačních schémat (z technického pohledu).

9. Vytvořit technickou příručku k aktivitám pro vytváření norem a definic specifikací v oblastech jako časové značky, bezpečná archivace, rozkrytí klíče (dle autorů materiálu se v těchto oblastech děje zatím málo).

C. Legislativní aspekty:

Zákony i normy jsou ve většině projektů široce akceptovány. Některé ryze operační projekty dříve zahájené zahájily práce na základě využívání proprietárních systémů, avšak následně (po přijetí odpovídajících norem a zákonů) přešly na systémy kompatibilní s formálními legislativními a normativními požadavky. Část však zůstává otevřeným problémem existence objektivního vyhodnocení této shody.

Doporučuje se zřetelně definovat takovou podmnožinu norem a zákonů, které dodavatelé musí splnit a dále vyhodnocovat tuto shodu.

Existují nedostatky vzhledem k řešení otázek ochrany soukromí v rámci struktur PKI, chybí patřičné normy.

Neexistují pojišťovací politiky, které by se týkaly aktivit spojených s digitálními certifikáty.

Doporučení.

1. Harmonizovat legislativní opatření v takových oblastech aplikací, jako elektronické identifikační karty, elektrické platby a digitální podpisy.
2. Zabezpečit harmonizaci a legislativní interoperabilitu mezi různými akreditačními schématy jednotlivých členských států. Urychlit v Evropě cesty k ekvivalentním akreditačním schématům. Využívat k tomu takové společné rámce jako je EESSI. Publikovat dokumenty, které ozřejmují společné body a naopak konfliktní momenty v návaznosti na Směrnici EU a potřeby trhu. Ověřit a identifikovat produkty kompatibilní s normami EESSI, pracovat na dostupnosti takových produktů na trhu.
3. Vytvořit průvodce k praktickým dopadům ochrany soukromí v PKI ve formě kombinace nejlepších praktických postupů a existující legislativy.
4. Vyvinout prostředky k analýzám cest pro úvěrování PKI projektů.
5. Ve spolupráci s odborníky na pojišťování připravit průvodce k definování vhodných pojišťovacích politik.

7. Materiály v příloze dokumentu

V příloze č.1 studie je uveden seznam kontaktovaných projektů. Celkem bylo kontaktováno 26 adresátů, pro studii byly dodány podklady, resp. bylo vybráno 11 projektů.

Zbývající oslovení adresáti:

- Austrian Citizen Identity Card
- Netherlands Citizen Identity Card
- France Sesame Vital (bez dalších informací, asi mimo rámec studie)
- Media@Komm Project, Germany (karty zdravotnického personálu)
- GTA (finanční systémy, Nizozemsko)
- Spanish office of Patents and Trade marks (bezpečný přístup k registrům a platby objednávek)
- Madrid Bar Association (notáři, Španělsko, autentizace odesilatele dokumentů)
- DigiNotar (notáři, Nizozemsko, třetí důvěryhodná strana)
- TTP.NL (akreditační schéma - Nizozemí)
- Tscheme (akreditační schéma ve velké Bitanii)
- Novotrust (firma nabizející SCPKI - Finsko)
- GISA, katalánský vládní projekt (elektronické podpisy smluv)
- Gov. of La Rioja, Španělsko (místní administrativa, podpisy dokumentů)
- Xunta of Galicia, Španělsko (bezpečný web, sociální zabezpeení, registrace smluv)
- Cities project - Marseille (experimentální projekt, občanské karty pro občany Marseille - zajištění on-line služeb zastupitelstva)
- Ministry of Agriculture, Španělsko (projekt zabývající se dokumentací k olivovým hájům)

V příloze 2. popisované studie je uveden dotazník s jehož pomocí byly získány uvedené informace.

D. Komparace českého zákona o elektronickém podpisu a slovenského zákona o elektronickom podpise s přihlédnutím k plnění požadavků Směrnice 1999/93/ES (II.část)

Jan Hobza, ÚOOÚ Praha

V minulém dílu jsme se zaměřili na odlišnosti českého a slovenského zákona v jejich působnosti a v definicích základních pojmů. O důsledcích subjektivní působnosti slovenského zákona se v tomto dílu již zmiňovat nebudeme. Vrátíme se ale k rozdílům českého a slovenského zákona v pojímání "běžných" a zaručených elektronických podpisů, protože tyto rozdíly mají zásadní důsledky a také se zaměříme na prokazatelnost času vytvoření elektronického podpisu.

Česká a slovenská právní úprava zaručeného (advanced [1]) elektronického podpisu ve smyslu Směrnice 1999/93/ES se zásadně liší. Slovenský zákon spojuje zaručený elektronický podpis s kvalifikovaným certifikátem. Pouze elektronický podpis založený na kvalifikovaném certifikátu může být označený jako zaručený. Oprávnění vydávat kvalifikované certifikáty má pouze akreditovaný poskytovatel. Jak tato situace odráží požadavky Směrnice 1999/93/ES ?

Směrnice neomezuje vydávání kvalifikovaných certifikátů pouze na akreditované poskytovatele. Dobrovolné akreditační systémy mají mít úlohu pouze zajištění vyšší úrovně poskytovaných služeb v rámci vybraných agend, nikoli roli jediných poskytovatelů kvalifikovaných certifikačních služeb (viz preambule a článek 3 Směrnice). Směrnice sice vyžaduje, aby kvalifikované elektronické podpisy [1,2,3] bylo možné z právního hlediska považovat za rovnocenné vlastnoručním podpisům za předpokladu, že jsou naplněny požadavky na vlastnoruční podpisy. Zároveň ale požaduje, aby státy nebránily poskytovatelům působit mimo rámec akreditačních schémat a aby tyto neomezovaly soutěž v oblasti certifikačních služeb. Pokud tedy zákony umožňují vytváření právně rovnocenných elektronických podpisů pouze na základě služeb akreditovaných poskytovatelů (tedy na základě určité formy licence), dostávají se do rozporu s požadavky Směrnice[1].

Na druhé straně od zaručeného elektronického podpisu stojí podle slovenského zákona "běžný" elektronický podpis. Ten může podle § 3 odst. 1 sloužit jen jako prostředek ověření integrity dokumentu. Mezi těmito instituty je prázdné místo, zákon jinou formu elektronického podpisu nedefinuje a novelizované zákony (občanský zákoník, správní řád aj.) připouští jen zaručený elektronický podpis. Ač se taková úprava může zdát dosti diskriminující vůči běžným certifikačním autoritám (na základě jejich služeb je možné vytvářet jen běžné elektronické podpisy, které neslouží jako prostředek autentizace podepisující osoby podle tohoto zákona - viz minulý díl), slovenský zákon se vyhýbá nedostatkům českého zákona při implementaci článku 5.2 Směrnice[1].

Český občanský zákoník v § 40 odst. 3 říká, že je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů. Těmito předpisy se rozumí zákon č. 227/2000 Sb., o elektronickém podpisu, protože v našem právním řádu je jediným zákonem, který upravuje náležitosti používání elektronického podpisu. Ten v § 3, který je nazván "Soulad s požadavky na podpis" říká, že datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pojem elektronický podpis je definován tamtéž v § 2 písm. a), kde se definuje, že elektronický podpis jsou údaje v elektronické podobě, které jsou připojené nebo jinak logicky spojené s datovou zprávou a

umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Elektronickým podpisem tedy mohou být i iniciály v textu e-mailové zprávy [4]. Podle mého názoru tedy je možné argumentovat, že právní úkon je podle českého občanského zákoníku možné platně elektronicky podepsat i připojením jména podepisující osoby za text datové zprávy. Příčinou tohoto názoru, který doufám vyvrátí příslušné judikáty či lépe novela zákona, je patrně snaha zákonodárce o přisouzení určité váhy elektronickým podpisům, které nejsou kvalifikovanými podpisy.

Jak vidíme, ani český, ani slovenský zákon o elektronickém podpisu nezachází s pojmy elektronický podpis a zaručený elektronický podpis v souladu s požadavky Směrnice. Slovenský zákon podle mého názoru omezuje trh certifikačních služeb na akreditované certifikační autority, protože pouze jejich kvalifikované certifikáty budou použitelné v souladu s platnými předpisy a degraduje úlohu běžných certifikačních autorit, kterým pouze ukládá nové povinnosti. Český zákon o elektronickém podpisu (mimo jiné) vzbuzuje teoretické pochybnosti o adekvátní formě elektronického podpisu pro zachování písemné formy právního úkonu.

Slovenský zákon upravuje i platnost zaručeného elektronického podpisu. Odvozuje ji i od prokazatelnosti doby jeho vytvoření, resp. od prokazatelnosti toho, že příslušný kvalifikovaný certifikát byl v době jeho vytvoření platný. Přesnou dobu platnosti certifikátu je jednoduché určit z intervalu platnosti certifikátu a případně z okamžiku zneplatnění certifikátu - zveřejnění CRL. Obtížnější může být určení okamžiku vytvoření podpisu. Jakým způsobem má být čas jeho vytvoření určen již zákon přímo nestanoví . Zákon zároveň neimplikuje neplatnost podpisu, pokud by tato doba nebyla prokazatelná. Při výkladu prokazatelnosti času vytvoření podpisu bychom se mohli opřít o vyhlášky slovenského Národního bezpečnostního úřadu, který byl zmocněn k provedení některých ustanovení zákona o elektronickém podpisu. Návrhy těchto vyhlášek je již možné najít na internetu na následující adrese http://www.nbusr.sk/index.php?menu=11 [5]. Vyhláška o vytvoření a ověření elektronického podpisu a časového razítka rozlišuje čtyři formy zaručeného elektronického podpisu, přičemž jeho tři vyšší formy jsou spojeny s časovým razítkem. V těchto případech je určení přesného okamžiku vytvoření podpisu jednoznačné, protože časové razítko, při splnění určitých zásad, je dobrým důkazem existence "orazítkovaných" dat před časem v něm uvedeným [6]. V případě zaručeného elektronického podpisu bez časového razítka bude záviset výše zmíněná prokazatelnost podle § 4 odst. 2 slovenského zákona buď na soudu (při řešení případného sporu) nebo na dohodě zúčastněných stran. Tato koncepce tedy umožňuje legální používání zaručeného elektronického podpisu jak s časovým razítkem, tak bez něj. To bezesporu patří k přednostem slovenského zákona před českým zákonem o elektronickém podpisu, který se určením času vytvoření podpisu vůbec nezabývá.

Český zákon a slovenský zákon o elektronickém podpisu se liší v mnoha dalších ohledech, které již nepovažuji za tolik zásadní. Jistě by bylo možné diskutovat o opodstatněnosti úpravy práv a povinností registračních autorit, o rozdílech v provádění dozoru a ukládání pokut, o nekonzistentní terminologii českého zákona apod., ale tyto diference jsou ve srovnání s výše uvedenými již marginální.

Na závěr bych si dovolil malou poznámku k důvodové zprávě ke slovenskému zákonu. Nejen v ní, ale i v mnoha dalších publikacích [např. 6] se uvádí, že přijetím zákona o elektronickém podpisu, případně přijetím prováděcích předpisů k tomuto zákonu, se "zrovnoprávňuje" elektronický podpis s vlastnoručním podpisem. Takovou domněnku je třeba apriori odmítnout. Slovenský zákon ani žádný jiný evropský zákon o elektronickém podpisu

toto neprovádí a Směrnice o elektronickém podpisu [1] to také nevyžaduje. Zásadním požadavkem Směrnice je, aby kvalifikované elektronické podpisy splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě stejně, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k datům na papíře. Co to vlastně znamená? Tam, kde právní předpis umožňuje činit právní úkony i v elektronické podobě, kvalifikovaný podpis má mít stejné právní účinky (předpoklad platnosti právního úkonu).

Z tohoto požadavku nevyplývá, že kvalifikovaný podpis má být rovnoprávným substitutem vlastnoručního podpisu, jako náležitost písemné formy právního úkonu. Právní řády členských států, ale i náš právní řád, vyžadují pro různé oblasti práva různou formu a různé podmínky právního úkonu. A tak i kvalifikovaný elektronický podpis lze platně použít pouze tam, kde to zákon připouští.

Pokud tedy občanský zákoník stanoví, že "vlastnoruční závěť musí být vlastní rukou napsaná a podepsaná, jinak je neplatná", nic vám nepomůže elektronický podpis. Kde se tedy můžeme platně elektronicky podepisovat? Všude tam, kde to právní předpis dovoluje (respektive neimplikuje neplatnost nedodržením písemné formy). Jsou to tedy takové úkony, které činíme podle § 34 až 51 občanského zákoníku (např. spotřebitelské smlouvy, kupní smlouvy, ale i smlouvy o dílo apod.). Dále je možné platně elektronicky učinit podání podle správního řádu, zákona o správě daní a poplatků, občanského soudního řádu či trestního řádu.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
http://www.volny.cz/honzahobza/Directive.pdf

[2] Policy requirement for certification authorities issuing qualified certificates TS 101 456

[3] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

[4] MATEJKA, Ján. Úprava elektronického podpisu v právním řádu ČR. Právník 5/2001

[5] Vyhlášky v době psaní tohoto textu ještě nebyly vydány ve slovenské sbírce zákonu, ale prošly již mezirezortním připomínkovým řízením a jsou dostupné na adrese:
http://www.nbusr.sk/index.php?menu=11.

[6] ŘEZNÍČEK, Ladislav. Rovnoprávnost. EURO, 1/2002. Též
http://www.epodpisy.cz/index.php?template=rs.html&id=136.

E. Komentář k článku pana RNDr. Tesaře : Runs Testy

RNDr. Luděk Smolík, seculab s.r.o. (lsmolik@web.de)

V článku „Runs Testy“ v čísle CW 2/2002 jsme se dočetli o statistických testech pro hodnocení výskytu sérií identických bitů v posloupnosti náhodných bitů. Recepty různých uvedených pramenů se zjevně liší v definici teoretických veličin. Rekapitulujeme zde krátce ještě jednou princip testů:

- Pod pojmem série rozumíme řadu následujících bitů stejného druhu (po sobě následující nuly nebo jedničky). Pravděpodobnost *p(i)* pro vznik řady posloupných *i* bitů stejného druhu je daná formulí:

$$p(i) = \frac{1}{2^i} \qquad (1)$$

  za předpokladu, že pravděpodobnost pro výskyt stavu „0“ a nebo „1“ je právě ½ a že mezi následujícími bity neexistuje žádná korelace. Teoreticky očekávaný počet sérií délky *i* můžeme definovat jako:

$$E'(i) = \widetilde{R}(N) \cdot p(i) \qquad (2)$$

  kde $\widetilde{R}(N)$ je očekávaný střední počet sérií v bitové posloupnosti délky *N*.

- V článku pana Tesaře jsou referovány dvě práce [1], [2] s podstatně odlišnými výsledky pro $E(i)$:

$$E(i) = N/2^{i+2} = \frac{1}{2} N/2^{i+1} \qquad (3) \text{ reference [1]}$$

$$E(i) = (N-i+3)/2^{i+2} = \frac{1}{2}(N-i+3)/2^{i+1} \qquad (4) \text{ reference [2]}$$

Kde je pravda?

Zdá se mi, že pravda leží jako obvykle někde uprostřed, jinak řečeno***, oba uvedené zdroje nemají pravdu!***

Pro důkaz tohoto tvrzení lehce modifikujeme a interpretujeme nejprve obě rovnice. Faktor ½ se v obou formulích (3) a (4) objevuje jako následek předpisu pro výpočet chí-kvadrátové funkce, v které se rozlišuje mezi počtem sérií jedniček a počtem sérií nul. Teoretický počet obou druhů sérií délky *i*, jak nulových tak jedničkových je tedy právě dvojnásobný:

$$E'(i) = 2 \cdot E(i) = 2 \cdot N/2^{i+2} = \frac{N}{2} \cdot \frac{1}{2^i} \qquad (5)$$

a pro referenci [2] :

$$E'(i) = 2 \cdot E(i) = 2 \cdot (N-i+3)/2^{i+2} = \frac{N-i+3}{2} \cdot \frac{1}{2^i} \qquad (6)$$

Srovnáme-li oba výsledky s rovnicí (2), můžeme identifikovat teoreticky očekávaný počet sérií $\widetilde{R}(N)$. Najdeme *N*/2 pro referenci [1] a $(N-i+3)/2$ pro referenci [2]. U druhého výsledku již sama o sobě zarazí závislost na proměnné *i*. Výsledky můžeme testovat pro přehledné příklady, třeba pro $N=2$. Očekáváme $\widetilde{R}(2) = (2 \cdot 1 + 2 \cdot 2)/4 = 1.5$ pro možné případy: 00, 11, 01 a 10.

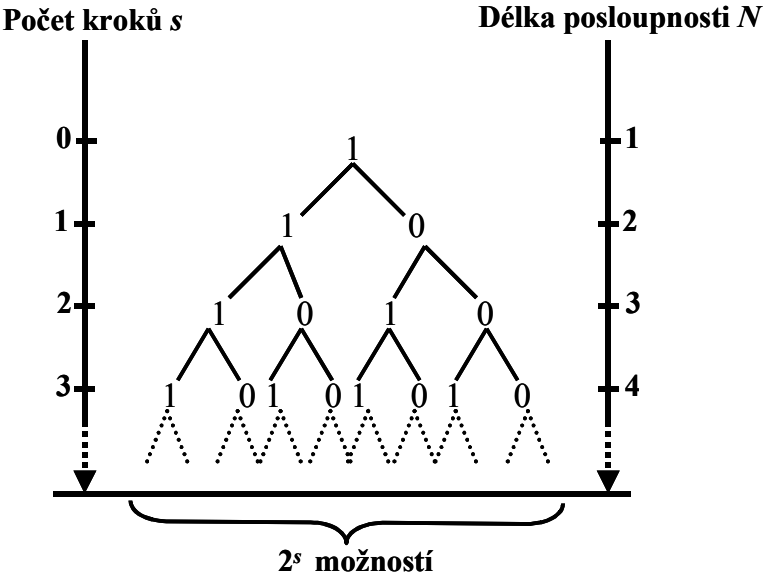
Pro referenci [1] obdržíme $\widetilde{R}(2) = 2/2 = 1$, a pro referenci [2] $\widetilde{R}(2) = (5-i)/2$ neobdržíme vlastně nic rozumného, protože co podniknout s proměnnou *i* ? V každém případě jsou oba výsledky zjevně chybné. A co platí pro malé *N* bude platit i pro velké hodnoty.

Položil jsem si druhou otázku, nedá se to opravdu spočítat?
Myslím že dá. Bez pomoci velké matematiky se dá doslova „z břicha“ najít formule pro $\widetilde{R}$.

Pohlédneme nejprve na oba extrémní případy. *Minimální* počet sérií, které mohou nastat, je právě jedna série, v které jsou všechny bity identické (00000..... a nebo 1111.....). Série má délku *N*. Na druhé straně je *maximálni* počet sérií právě *N*. Každá série má délku jeden bit (0101..... a nebo 1010.....). Střední očekávaná hodnota bude tedy ležet někde mezi 1 a *N* a jelikož se tento problém zdá být zcela symetrický, nic nám nebrání stanovit hypotézu: $\widetilde{R}(N)$ je aritmetický střed mezi 1 a *N* .

$$\widetilde{R}(N) = \frac{N+1}{2} \qquad (7)$$

Pro důkaz tohoto tvrzení pohlédneme na obrázek 1, který ukazuje vznik možných sérií. Zvolíme první bit (nultý krok) „1“. Při každém následujícím kroku máme možnost volby mezi „0“ a „1“ se stejnou pravděpodobností ½.. Po *s* krocích jsme prošli strom možností jednou možnou cestičkou a obdrželi jsme posloupnost délky $N = s+1$ bitů. Tato posloupnost má *k* sérií. Kupříkladu „1100“, pro $N = 4$ a $k = 2$. Pohlédneme-li na obrázek 1, najdeme více možných cestiček, které dávají $k = 2$, totiž „1110“ a „1000“. (Při volbě „0“ jako první bit, by byl výsledek zcela symetrický strom , tak jako na obrázku 1 a našli bychom tři další možnosti: „0011“, „0001“ a „0111“. Zároveň se ale zdvojnásobí počet všech možností. Na následující argumentaci se ale nic nemění.)



Obrázek 1: Strom možností pro počáteční bit „1“

Počet možností *M* pro výskyt právě *k* sérií po $s = N - 1$ krocích je dán vzorcem:

$$M(k) = \binom{s}{k} \tag{8}$$

Korespondující pravděpodobnost *m* obdržíme z (8) dělením počtem všech možností po *s* krocích (v. obrázek 1).

$$m(k) = \frac{M(k)}{2^s} = \binom{s}{k} \cdot \frac{1}{2^s} = \binom{s}{k} \cdot \left(\frac{1}{2}\right)^k \cdot \left(\frac{1}{2}\right)^{s-k} \tag{9}$$

Ve výsledku rozeznáme dobře známou binomiální formuli pro pravděpodobnost ½. Očekávaná střední hodnota $\widetilde{R}$ pro binomiální rozložení je daná (např. podle [3]):

$$\widetilde{R}(s) = \sum_{k=1}^{s} k \cdot m(k) = \sum_{k=1}^{s} k \cdot \binom{s}{k} \cdot \left(\frac{1}{2}\right)^k \cdot \left(\frac{1}{2}\right)^{s-k} = s \cdot \frac{1}{2} \tag{10}$$

Použijeme vztah $s = N - 1$ a dostaneme:

$$\widetilde{R}(s) = \widetilde{R}(N-1) = \frac{N-1}{2} \tag{11}$$

Tato rovnice platí samozřejmě pouze pro $N \geq 2$. Pro $N = 1$ snadno realizujeme, že platí $\widetilde{R}(1) = 1$. Nakonec použijeme větu: očekávaná hodnota sumy se rovná součtu jednotlivých očekávaných hodnot a obdržíme konečně:

$$\widetilde{R}(N) = \widetilde{R}(1 + N - 1) = \widetilde{R}(1) + \widetilde{R}(N-1) = 1 + \frac{N-1}{2} = \frac{N+1}{2}$$

Quod erat demonstrandum !

Samozřejmě platí nadále pro velké *N* a pro malé *i* :

$$N/2 \approx (N - i + 3)/2 \approx (N+1)/2$$

[1] Maurer, U.M.: "An Universal Statistical Test for Random Bit Generators", Journal of Cryptology, Vol 5, No. 2, 1992

[2] Menezes, A.J., Oorschot, P.C., Vanstone, S.A., "Handbook of Applied Cryptography", CRC Press, 1997

[3] Bronstein I.N., Semendjajew K.A., "Taschenbuch der Mathematik", Verlag Nauka Moskau, Teubner Verlagsgesellschaft, Leipzig

F. Konference

ICZ zakládá tradici konferencí o bezpečnosti

První ročník konference BIN (Bezpečnost informací) 2002 se konal v Praze v hotelu Diplomat. Společnost ICZ a.s. zvolila pro konání konference symbolické datum - 11. září, chtěla tím podtrhnout význam bezpečnosti v současném světě. Firma hodlá založit každoroční tradici setkávání odborníků v oboru, řešitelů i uživatelů, lidí z teorie i praxe. Pěkné prostředí, zcela zaplněná přednášková místnost a hodnotné přednášky jsou jistě dobrým vykročením pro uskutečnění tohoto záměru.

K výběru přednášejících a obsahu příspěvků prvního ročníku BIN 2002 přistoupila pořádající společnost ICZ v duchu firemní filozofie mnohovrstevného přístupu k řešení bezpečnosti informací včetně schopnosti poskytnout jak služby strategického charakteru, tak konkrétní technická resp. legislativní řešení.

Přednášky byly rozděleny do několika samostatných bloků. První blok byl věnován elektronickému podpisu a kryptologii. Zde zazněly přednášky „Elektronický podpis prakticky“ (RNDr. Vlasta Jošková , ICZ, Mgr.Pavel Vondruška, ÚOOÚ), „Elektronická podatelna – nic jednoduchého“ (Ing. Pavel Staša , ICZ), „Elektronický vs. vlastnoruční podpis – co je bezpečnější?“ (JUDr. Ján Matejka, Ústav státu a práva AV ČR). Posluchači tak získali základní informace o pojmech zákona o elektronickém podpisu, souvisejících právních předpisech, nárocích na zavádění elektronického podpisu a získali i informace o odpovědnosti a povinnostech jednotlivých subjektů jako jsou podepisující osoba, osoba spoléhající na podpis a poskytovatel certifikačních služeb. Ohlas na tyto přednášky prokázal, že téma elektronického podpisu a jeho zavádění do praxe je velice aktuální a o tuto oblast mají posluchači velký zájem. Kryptologové pořádající firmy RNDr. Vlastimil Klíma a Ing. Tomáš Rosa prezentovali své vlastní vysoce hodnotné výsledky v bouřlivě se vyvíjející nové části kryptologie, která se zabývá tzv. postranními kanály, které nežádoucím způsobem vynáší důležité informace z informačních systémů. Svůj příspěvek nazvali „Postranní kanály – moderní hrozby informačních a komunikačních systémů“

Odpolední blok byl věnován klasickým otázkám bezpečnosti. RNDr. Ivan Svoboda, CSc. ze společnosti Oracle přednesl aktuální příspěvek „Příprava na zvládání havarijních situací v informačních systémech“. Podtrhl skutečnost, že stále jen málokterá organizace si skutečně uvědomuje důležitost svých dat a jejich ochrany. Příspěvek „Zásady a postupy při zajišťování personální bezpečnosti“ přednesl Ing. Jaroslav Mejstřík z ČNB. Posledním přednášejícím byl Ing. Ondřej Felix, CSc., předseda představenstva Českého Telecomu. Tento zkušený odborník ve svém velmi zajímavém příspěvku zdůraznil nutnost zabývat se praktickými otázkami bezpečnosti, nutnost správně balancovat mezi rizikem a cenou, ale především zdůraznil faktor důvěry ve společnost – tedy faktor, který z hlediska firmy lze jen těžko ocenit. V příspěvku připomenul účinnost bezpečnostních opatření a vysokou úroveň krizových plánů Českého Telecomu, kterou společnost prokázala během nedávných povodní.

Další informace lze najít na stránce konference http://www.i.cz/bin2002

ECOM-MONITOR.COM

Mikulášská kryptobesídka

2. – 3. prosinec 2002, Praha

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop zaměřený na podporu úzké spolupráce odborníků pracujících na poli aplikované kryptografie a v příbuzných oblastech bezpečnosti, se koná za účelem podpory výměny informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez zbytečných problémů a starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop navazuje na úspěšná setkání Velikonoční kryptologie 3.-4.4.2002 v Brně a Mikulášskou kryptobesídku, která se konala 10.-11.12.2001 v Praze. Workshop se skládá z (a) neformálního setkání (a případně panelové diskuse) v pondělí *2. prosince 2002* a (b) prezentací příspěvků a diskusí v úterý *3. prosince 2002*.

Na workshopu budou předneseny dva zvané příspěvky:
Vincent Rijmen (Cryptomathic, Belgie) o kryptoalgoritmech Rijndael/AES a jeho úpravě Anubis,
Geraint Price (Royal Holloway a PricewaterhouseCoopers, UK) o možnostech PKI.

Pokyny pro autory

Zájemci mohou poslat své příspěvky zaměřené především na oblast aplikované kryptografie, ale i bezpečnostních aplikací kryptografie a dalších oblastí kryptografie. Šablony (Word a LaTeX) pro přípravu příspěvků lze stáhnout ze stránky
http://www.ecom-monitor.com/kryptobesidka/cfp.html .

Návrhy příspěvků (5-15 stran A4) bez uvedení informací o autorech a zjevných odkazů, s oddělenou stranou textu s autorovou emailovou adresou, telefonním číslem a poštovní adresou, musí programový výbor (PV) obdržet na níže uvedené adrese nejpozději do *22. října 2002*. Elektronická podání jsou preferována; papírová podání musí obsahovat 7 vytištěných kopií.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *1.listopadu*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), před *18. listopadem*. Příspěvky mohou být napsány v češtině, slovenštině nebo angličtině.

Rozšířené abstrakty i kompletní příspěvky by měly být odeslány v RTF, HTML nebo ASCII.

Zasílání příspěvků

Preferujeme elektronické podání příspěvků.
E-mail: *Vaclav.Matyas@ecom-monitor.com*
Předmět: "MKB 2002"
Poštovní adresa: ***V. Matyáš***
ecom-monitor.com, a.s.
PO Box 7
664 01 Bílovice nad Svitavou

Důležitá data

Podání návrhů příspěvků:	21. října 2002
Oznámení o přijetí/odmítnutí:	5. listopadu 2002
Pracovní verze příspěvků:	21.listopadu 2002
Workshop:	2. – 3. prosince 2002š
Podání finálních příspěvků:	11. ledna 2003

Programový výbor

Tonda Beneš, SAP ČR a UK Praha
Petr Hanáček, VUT Brno
Vašek Matyáš, ecom-monitor.com a MU Brno
Daniel Olejár, UK Bratislava
Tomáš Rosa, ICZ a ČVUT Praha
Pavel Vondruška, ÚOOÚ
Jozef Vyskoč, VaF Bratislava

Organizační výbor

Dan Cvrček, VUT Brno
Jaroslav Dočkal, Vojenská akademie Brno
Magda Procházková, ecom-monitor.com
Zdeněk Říha, ecom-monitor.com a MU Brno
Jan Staudek, MU Brno
Eva Špatná, ecom-monitor.com – tajemnice
Petr Švéda, MU Brno

DATAKON 2002 - pozvání k účasti

Databázová konference, 19. - 22. 10. 2002, Hotel SANTON, Brno

podrobné informace -> http://www.datakon.cz/
datum včasné registrace na konferenci**: 20.9.2002** !

DATAKON je prestižní česká a slovenská konference s mezinárodní účastí zaměřená na teoretické a technické základy, nejlepší postupy a vývojové trendy v oblasti využití informačních technologií při budování informačních systémů včetně výsledků jejich aplikace v praxi.
DATAKON představuje ideální platformu pro výměnu zkušeností mezi českými i zahraničními odborníky z řad dodavatelů informačních technologií, jejich zákazníků a akademického světa.
DATAKON oslovuje zkušené odborníky i nejlepší studenty.

Tématické okruhy

Architektury databázových aplikací, bezpečnost informačních systémů, datové sklady a OLAP, formální specifikace software, geografické informační systémy, integrace heterogenních informačních zdrojů, Java a databáze, konverze a migrace dat, metadata, ontologie, modelovaní informačních zdrojů v prostředí internetu, multimedialní databáze, normy a standardy, objektové relační databáze, jejich modelování a návrh, objevovaní znalosti a data mining, právní aspekty manipulace s informacemi, služby internetu/intranetu a databáze, správa a ladění databází, XML a databáze, workflow, znalostní databáze

---

Organizují

Česká informatická společnost, pobočka Brno
Česká společnost pro systémovou integraci
Fakulta elektrotechnická, CVUT Praha
Fakulta elektrotechniky a informatiky, STU Bratislava
Fakulta informatiky, MU Brno
Fakulta informatiky a statistiky, VSE Praha
Matematicko-fyzikální fakulta, UK Praha
Slovenska informatická společnost

Programový výbor DATAKON 2002 (členové viz www.datakon.cz)
Organizační výbor DATAKON 2002 (členové viz www.datakon.cz)
Kontaktní adresa - datakon@datakon.cz
Sponzoři a mediální partneři - viz www.datakon.cz
Platby a registrace - viz www.datakon.cz

G. Letem šifrovým světem

1. Zveřejněn nový standard pro hashovací funkce

Federal Information Processing Standards Publications (FIPS PUBS) , které vydává National Institute of Standards and Technology (NIST), zveřejnil 1.srpna 2002 standard Secure Hash Signature Standard (SHS) (FIPS PUB 180-2). Tento standard patří do kategorie Computer Security Standard, Cryptography. Jsou v něm specifikované čtyři bezpečné hashovací algoritmy SHA-1, SHA-256, SHA-384 a SHA-512. Pro zprávy délky $< 2^{64}$ bitů jsou určeny algoritmy SHA-1 a SHA-256. Zbývající dva algoritmy SHA-384 a SHA-512 jsou určeny pro zprávy délky $< 2^{128}$ bitů. Délka výstupu (tzv. message digest) závisí na typu zvoleného algoritmu a pohybuje se od 160 bitů do 512 bitů. Hashovací algoritmy se používají např. při výpočtu digitálních podpisů, generování náhodných čísel nebo při vytváření autentizačních kódů závislých na klíči. Tento standard nahrazuje dosud platný standard FIPS 180-1, který obsahoval popis pouze jediného bezpečného hashovacího algoritmu SHA-1. Standard je závazný pro využití ve „vládních" aplikacích USA a to pro využití v kryptografických algoritmech a protokolech. Jeho použití v soukromé a komerční sféře má doporučující charakter. Standard bude uplatňován od 1.února 2003.
V elektronické podobě jej lze získat na adrese : http://csrc.nist.gov/publications/ .

2. Korejská společnost Beaucom přivádí do mobilního světa dva nové modely **mobilních telefonů s vestavěným dodatečným šifrováním** - Tresor (model určený pro vývoz do Anglie a Ruska) a Enigmu (určen pro Německo). Tyto telefony, které mají zabránit odposlechu (třeba i policejnímu), nejsou drahé a budou pravděpodobně dováženy i do ČR.
http://www.mobil.cz/mobilni_komunikace/mobilni_telefony/abecedni_prehled_mt/ostatni/beaucom020911.html

3. Nový, rychlejší **algoritmus určený pro testování,** zda dané číslo je nebo není **prvočíslo,** najdete zde : http://www.cse.iitk.ac.in/news/primality.pdf .

4. V archivu IACR je k dispozici příspěvek, který obsahuje nový krypto-analytický výsledek týkající se algoritmu **Rijndael**. Nejedná se o nový typ útoku, ale je zde popsána nová matematická vlastnost této šifry. Tato vlastnost nebyla dříve známa a tedy při bezpečnostní analýze ještě nebyla vzata do úvahy. http://eprint.iacr.org/2002/111/

5. Česká pošta začala nabízet **registrovanou elektronickou poštu**, která může nahradit doporučený dopis. O tuto digitální službu již projevily zájem zdravotní pojišťovny a nemocnice, které měsíčně zpracovávají tisíce soupisů lékařských výkonů a dosud je musely zasílat na disketách v doporučených zásilkách. Podle mluvčího pošty Ladislava Vančury stačí k využití služby jednorázový poplatek za elektronickou schránku na datových serverech pošty. Při zasílání zprávy elektronickou cestou pošta prověří totožnost odesílatele i adresáta na základě **elektronického podpisu**, který již pro všechny stálé zákazníky ve vnitřním systému pošty funguje. Pokud adresát zásilku přijme, obdrží odesílatel elektronickou doručenku podobnou klasické papírové doručence. Informace o doručení bude uložena na chráněných serverech.
Zaváděním elektronických služeb se Česká pošta snaží konkurovat rychlému rozvoji Internetu a rostoucímu počtu mobilních telefonů.

6. O čem jsme psali v září v letech 1999 - 2001

Crypto-World 9/1999

http://www.mujweb.cz/veda/gcucmp/Casop1/Crypto09_99.zip/

Crypto-World 9/2000

http://www.mujweb.cz/veda/gcucmp/Casop2/Crypto09_00.zip/

+ příloha : gold_bug.rtf
Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

http://www.mujweb.cz/veda/gcucmp/Casop3/Crypto09_01.zip/

H. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprochází jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :
http://www.mujweb.cz/veda/gcucmp

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
vondruska.p@seznam.cz
pavel.vondruska@post.cz