Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 3/2003 **17. březen 2003**

3/2003

Připravil : Mgr.Pavel Vondruška

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

(413 e-mail výtisků)

Obsah : **Str.**

Příloha : crypto_p3.pdf
Mezinárodní a zahraniční normalizační instituce
(články neprocházejí jazykovou korekturou)

A. České technické normy a svět, III.část

Pavel Vondruška, ČESKÝ TELECOM, a.s.

3. Mezinárodní vztahy

ČSNI udržuje rozsáhlé styky s mezinárodními a evropskými normalizačními organizacemi a s národními normalizačními organizacemi řady zemí. Jako nástupce dřívějších čs. normalizačních orgánů je řádným členem za Českou republiku v Mezinárodní normalizační organizaci (ISO) a Mezinárodní elektrotechnické komisi (IEC).

Na evropské úrovni je od roku 1997 plnoprávným řádným členem Evropského výboru pro normalizaci (CEN) a Evropského výboru pro elektrotechnickou normalizaci (CENELEC) a to se všemi právy a povinnostmi. Povinností je uskutečnění připomínkového řízení ke všem návrhům norem, obhájení připomínek na jednáních technických komisí a hlasování o konečném znění evropských norem. Další povinností je zavedení evropských norem do národní soustavy norem a to v půlročním termínu.

Přehled vybraných dokumentů CEN můžete nalézt v příloze crypto_p1.pdf k Crypto-Worldu 1/2003.

ČSNI má v Evropském telekomunikačním normalizačním institutu (ETSI) statut pozorovatele. Přehled dokumentů ETSI, které se zabývají elektronickým podpisem, je uveden v příloze crypto_p2.pdf k Crypto-Worldu 2/2003.

Mezinárodní normalizační spolupráce se realizuje účastí ČSNI na tvorbě evropských a mezinárodních norem v pracovních orgánech normalizačních organizací. ČSNI dále zabezpečuje některá zasedání technických komisí popř. subkomisí v ČR a má své zástupce v řídících orgánech (Technickém řídícím výboru, Správní radě apod.) CEN/CENELEC.

Elektronická výměna dat s mezinárodními organizacemi a zpracovateli se uskutečňuje klasickými metodami přenosu dat na disketách nebo CD-ROM nebo pomocí satelitního příjmu a stále častěji pomocí Internetu.

Přehled nejvýznamnějších mezinárodních a zahraničních normalizačních organizací uvádím v příloze crypto_p3.pdf k tomuto číslu Crypto-Worldu.

3.1 Mezinárodní organizace pro normalizaci (ISO)

ISO je celosvětovou federací 130 národních normalizačních orgánů, je nevládní organizací a byla založena v roce 1947.

Posláním ISO je podporovat rozvoj standardizace ve světě a tím usnadnit mezinárodní obchod a rozvíjení kooperace ve sféře intelektuální vědecké, technologické a ekonomické aktivity. Výsledkem činnosti ISO jsou mezinárodní standardy, které obvykle připravují technické komise ISO.

Členové ISO jsou rozděleni do tří kategorií:

1. „Member body of ISO“

Plnoprávným členem ISO je vždy jen jedna organizace z konkrétního státu, která ho v oblasti standardizace nejvíce reprezentuje. Člen ISO musí informovat potenciální zájemce ve

své zemi o mezinárodních normalizačních aktivitách, zastupovat státní zájmy v jednáních ISO vedoucích k ustanovení mezinárodních standardů a platit členské poplatky. Účastní se jednání v technických komisích ISO a má hlasovací právo.

2. „Correspondent member"

Sem patří organizace zastupující státy, které ještě nemají plně rozvinutou standardizační infrastrukturu. Neúčastní se aktivně jednání, ale jsou o dění v ISO informovány.

3. „Subscriber membership"

Pod tento typ členství byly zařazeny státy s nerozvinutou ekonomikou. Platí nízké členské poplatky, které jim i přesto umožňují udržovat kontakt s mezinárodní standardizací.

ISO je decentralizovaná instituce, tvořená 2 850 technickými komisemi, podkomisemi a pracovními skupinami. Komise tvoří zástupci průmyslu, výzkumných ústavů, spotřebitelů a mezinárodních organizací z celého světa a jako rovnocenní partneři se setkávají na jednáních ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této komisi zastoupen. Práce se zúčastňují také vládní i nevládní neziskové organizace, s nimiž ISO navázala pracovní styk.

Centrální sekretariát ISO se nachází v Ženevě. Stará se o to, aby dohody schválené technickými komisemi byly editovány, vytištěny, předloženy k hlasování členům ISO a vydány. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů. Také svolává jednání komisí, datum a místo s nimi předtím konzultuje. Většina tvůrčí práce však probíhá korespondenčně.

Publikace *ISO Memento* poskytuje informace o činnosti každé z technických komisí. Podrobná pravidla pro práci na mezinárodních standardech jsou popsána v *ISO/IEC Directives*. V publikaci *ISO Liaisons* je seznam okolo 500 mezinárodních organizací, které spolupracují s technickými komisemi ISO.

ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice [1] .

3.2 Mezinárodní elektrotechnická komise (IEC)

IEC je celosvětovou mezinárodní organizací zahrnující všechny národní elektrotechnické komitéty (národní komitéty IEC) a byla založena v roce 1906. Cílem IEC je podporovat mezinárodní spolupráci ve všech otázkách, které se týkají normalizace v oblasti elektrotechniky a elektroniky. Za tím účelem, kromě jiných činností, IEC vydává mezinárodní normy. Jejich příprava je svěřena technickým komisím; každý národní komitét IEC, který se zajímá o projednávaný předmět, se může těchto přípravných prací účastnit. Mezinárodní vládní i nevládní organizace, s nimiž IEC navázala pracovní styk, se této přípravy rovněž zúčastňují.

IEC úzce spolupracuje s ISO v souladu s podmínkami dohodnutými mezi těmito dvěma organizacemi, s CENELEC (Evropský výbor pro elektrotechnickou normalizaci) a s ETSI (Evropský telekomunikační normalizační institut) [2].

IEC má více než 50 členů. Prvním typem členství je tzv. „*full membership*" neboli plné členství. Jedná se o národní organizace, které mají možnost se aktivně podílet na práci v IEC a mají volební právo. Druhým typem členství je tzv. *„associate membership"* neboli partnerské členství. V takovém případě mají národní organizace jen statut pozorovatele, to znamená, že se nepodílí aktivně na práci v IEC a nemají právo hlasovat.

Oficiální rozhodnutí nebo dohody IEC týkající se technických otázek připravených technickými komisemi, v nichž jsou zastoupeny všechny zainteresované národní komitéty, vyjadřují v nejvyšší možné míře mezinárodní shodu v názoru na předmět, kterého se týkají. Mají formu doporučení pro používání publikované prostřednictvím norem, technických zpráv nebo pokynů a v tomto smyslu jsou přijímány národními komitéty. Na podporu mezinárodního sjednocení tyto komitéty mezinárodní normy IEC transparentně v maximálně možné míře přejímají do svých národních a regionálních norem. Každý rozdíl mezi normou IEC a odpovídající národní nebo regionální normou se v těchto normách jasně vyznačí. IEC nemá žádný postup týkající se vyznačování schválení a nenese žádnou odpovědnost za prohlášení o shodě předmětu s některou jeho normou. [2]

3.3 Evropský výbor pro normalizaci (CEN)

Posláním CEN je podporovat dobrovolnou technickou harmonizaci v Evropě ve shodě s celosvětovými orgány a jejich partnery v Evropě.

Harmonizace ztenčuje obchodní bariéry, zvyšuje bezpečnost, umožňuje výměnu zboží, systémů a služeb a zvyšuje základní technické porozumění. V Evropě CEN spolupracuje s CENELEC (Evropský výbor pro elektrotechnickou normalizaci) a ETSI (Evropský telekomunikační normalizační institut).

CEN pracuje podle zásad, které mají zajistit následující:

- **otevřenost a průhlednost**
Všechny zainteresované společnosti se podílejí na práci. Zastoupení je chráněno především národními normalizačními orgány, které mají povinnost posílat vyvážené zprávy politickým orgánům a technickým výborům. Zástupci průmyslu a ostatních oblastí mají své zastoupení v politických výborech. Celý pracovní program je vydán v „*CEN´s Work programme*“.

- **konsensus**
Evropské normy jsou vytvořeny na základě svobodného souhlasu mezi všemi zainteresovanými členy.

- **národní výbor**
Formální přijetí evropských norem se rozhoduje prostou většinou hlasů ze všech národních členů a pro všechny je zavazující.

- **technická soudržnost na národní a evropské úrovni**
Normy tvoří soubor, který zajišťuje vlastní kontinuitu pro dobro uživatelů, a to jak na evropské úrovni, tak na národních úrovních a to díky závaznosti zavádění evropských standardů a stahování problematických národních norem.

- **správná integrace mezinárodní práce**
Normalizace je drahá a časově náročná.

Tvorbu norem provádí technické komise a subkomise. Koordinaci technických činností zajišťuje Technical Board CEN. Ročně se vypracuje v CEN zhruba 1000 evropských norem. Důležitá rozhodnutí jsou předkládána generálnímu shromáždění, které se schází 1x ročně. Generální shromáždění se dělí na dvě části. Veřejnou část, na kterou jsou pozváni zástupci jiných mezinárodních a regionálních organizací a kde jsou projednávány obecné otázky evropské normalizace, a uzavřenou část, kde jsou přítomni pouze zástupci národních normalizačních organizací řádných členů a přidružených členů CEN.

V září roku 1999 se poprvé konalo generální zasedání CEN i v Praze.

Členy CEN jsou národní normalizační organizace zemí Evropské unie a Evropského sdružení volného obchodu.

CEN lze dělit na následující členy:

- řádné národní

Své zastoupení v CEN mají státy: Rakousko (ON), Belgie (IBN/BIN), Česká republika (ČSNI), Dánsko (DS), Finsko (SFS), Francie (AFNOR), Německo (DIN), Řecko (ELOT), Island (STRÍ), Irsko (NSAI), Itálie (UNI), Lucembursko (SEE), Nizozemí (NEN), Norsko (NSF), Portugalsko (IPQ), Španělsko (AENOR), Švédsko (SIS), Švýcarsko (SNV), Velká Británie (BSI)

- spolupracující členy (asociace)

ANEC (European Association for the co-operation of consumer representation in standardization)
CEFIC (European Chemical Industry Council)
EUCOMED (European Confederation of Medical Devices Associations)
FIEC (European Construction Industry Federation)
NORMAPME (European Office of Crafts, Trades and Small and Medium-sized Enterprises for standardization)
TUTB (European Trade Union Technical Bureau for Health and Safety)

- poradní členy (evropské instituce)
EC (The European Commission - Evropská komise)
EFTA Secretariat (European Free Trade Association - Evropská asociace volného obchodu)

- přidružené (afiliované) členy

Tito členové se mohou stát řádnými členy po splnění všech podmínek stanovených CEN, mimo jiné musí zavést 80% evropských norem do svých národních technických norem.

Na přijetí do CEN čekají státy se zastoupením: Albánie (DPS); Bulharsko (SASM); Chorvatsko (DZNM); Kypr (CYS); Estonsko (ESK); Maďarsko (MSZT); Lotyšsko (LVS); Litva (LST); Malta (MSA); Polsko (PKN); Rumunsko (ASRO); Slovensko (SUTN); Slovinsko (SMIS) a Turecko (TSE).

3.4 Evropský výbor pro elektrotechnickou normalizaci (CENELEC)

CENELEC byl ustanoven roku 1973 jako nevýdělečně činná organizace v rámci belgického práva. Oficiálně byl uznán jako evropská normalizační organizace Evropskou komisí nařízením 83/189 EEC.

Od konce padesátých let spolupracují členové CENELEC na programu evropské harmonizace svých norem. CENELEC má 40 000 technických odborníků v 19 zemích Evropského společenství a EFTA (Evropské sdružení volného obchodu) pro vydávání norem pro evropský trh [3] .

Literatura

[1] http://www.iso.ch/infoe/intro.htm

[2] Metodické pokyny pro normalizaci MPN 1: 1999 : stavba, členění a úprava českých technických norem. 1. vyd. Praha : Český normalizační institut, 1999.

[3] http://www.cenelec.org/Info/about.htm

B. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem

Ing. Petr Wallenfels petr.wallenfels@csni.cz

Do 70tých let bylo používání bezpečnostních, zejména kryptografických technik určených na ochranu informací omezeno na specifické oblasti aplikace. S rozšířením osobních počítačů a počítačových sítí, s nástupem Internetu a prováděním obchodních i dalších činností on-line se tento stav dramaticky změnil. Prudce vzrostla rovněž možná rizika spojená s využíváním těchto progresivních technologií. Proto se začal zejména v posledních letech klást důraz na jejich bezpečnost, tj. na zajištění zejména integrity, důvěrnosti a dostupnosti dat zpracovávaných prostřednictvím těchto technologií. Je zřejmé, že normalizované bezpečnostní techniky (autentizace entit, integrita dat, nepopiratelnost, důvěrnost dat) se stávají povinnými požadavky pro elektronický obchod, zdravotní péči a řadu dalších aplikačních oblastí. Bezpečnost IT se tak stala s ohledem na svůj průřezový charakter významnou částí normalizačních aktivit v celém světě.

Mezinárodní organizace pro normalizaci ISO (International Organisation for Standardisation) vyvíjí normy týkající se bezpečnosti informačních technologií v několika svých komisích a subkomisích. Nejdůležitější jsou vyvíjené pod ISO/IEC JTC1 SC 27 (Informační technologie – Bezpečnostní techniky) a TC 68 (Bankovnictví a související finanční služby).

V oblasti spolupráce s ostatními normalizačními komisemi ISO je cílem zajistit vývoj společných norem, vyhnout se možnému. překrývání a duplicitám ve vyvíjených normách a sdílet expertizy. SC 27 úzce spolupracuje v oblasti bezpečnostních norem s TC 68; za tímto účelem byla zřízena společná koordinační komise. Další spolupráce s ITU-T SG 7/Q20 je zaměřena zejména na vydávání společných norem. Spolupráce s CCIMB (Common Criteria Interpretation Managerial Board) umožňuje národním úřadům, které nejsou členy CCEB (Common Criteria Editorial Board) a CCIMB revidovat, připomínkovat a přispívat k vyvíjeným projektům (např. Common Criteria).

Vzhledem k tomu, že vývoj bezpečnostních norem je velmi náročnou záležitostí nezpracovávají se původní české normy. Vzhledem k úkolům na úseku harmonizace norem a právních dokumentů jsou běžně mezinárodní bezpečnostní normy ISO národními normalizačními orgány přejímány a vydávány jako národní normy. ČSNI plní v této oblasti významnou roli– mezinárodní bezpečnostní normy mající charakter průřezových norem (vyvíjené ISO/IEC JTC1 SC 27) jsou průběžně sledovány, přejímány a vydávány a aktualizovány jako české technické normy již řadu let. ČSNI rovněž zajišťuje mezinárodní spolupráci v této oblasti.

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají problematiku bezpečnosti informačních technologií na průřezové úrovni, jsou tedy všeobecně využitelné. Zajišťují normalizaci generických metod a technik pro bezpečnost informačních technologií. To zahrnuje:

- identifikaci generických požadavků (včetně požadavků na metodologii) pro bezpečnostní služby systémů IT
- vývoj bezpečnostních technik a mechanismů (včetně registračních postupů a vztahů mezi bezpečnostními komponentami)

- vývoj bezpečnostních směrnic (např. interpretační dokumenty)
- vývoj dokumentace a norem určených k podpoře managementu (např. terminologie a kritéria pro hodnocení bezpečnosti, problematika analýzy rizik).

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají normalizaci kryptografických algoritmů pro zajištění služeb integrity, autentizace a nepopiratelnosti. Zahrnují rovněž normalizaci kryptografických algoritmů pro zajištění služeb důvěrnosti a to v souladu s mezinárodně akceptovanými zásadami.

Přehled ČSN z oblasti bezpečnosti informačních technologií

ČSN ISO/IEC	2382-1	Informační technologie - Slovník - Část 1: Základní termíny
ČSN ISO/IEC	2382-8	Informační technologie - Slovník - Část 8: Bezpečnost
ČSN ISO/IEC	2382-14	Informační technologie - Slovník - Část 14: Spolehlivost
ČSN ISO/IEC	10116	Informační technologie - Bezpečnostní techniky - Módy činnosti pro n-bitovou blokovou šifru
ČSN ISO/IEC	10118-1	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně
ČSN ISO/IEC	10118-2	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající n-bitovou blokovou šifru
ČSN ISO/IEC	10118-3	Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované hash funkce
ČSN ISO/IEC	10118-4	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku
ČSN ISO	10126-1	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - Část 1: Obecné zásady
ČSN ISO	10126-2	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 2: Algoritmus DEA
ČSN ISO	10202-1	Identifikační karty. Karty pro finanční transakce. Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody. Část 1: Životní cyklus karty
ČSN ISO	11131	Bankovnictví - Autentizace přihlášením
ČSN ISO	11166-1	Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů - Část 1: Zásady, postupy a formáty
ČSN ISO	11166-2	Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 2: Schválené algoritmy používající kryptosystém RSA
ČSN EN ISO	11568-1	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů
ČSN EN ISO	11568-2	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru
ČSN EN ISO	11568-3	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus klíče pro symetrickou šifru
ČSN ISO/IEC	11770-1	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura
ČSN ISO/IEC	11770-2	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	11770-3	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ČSN ISO/IEC TR	13335-1	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT
ČSN ISO/IEC TR	13335-2	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT
ČSN ISO/IEC TR	13335-3	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT
ČSN ISO/IEC TR	13335-4	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření
ČSN ISO/IEC	13888-1	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně
ČSN ISO/IEC	13888-2	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	13888-3	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC	14888-1	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně
ČSN ISO/IEC	14888-2	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě
ČSN ISO/IEC	14888-3	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu
ČSN ISO/IEC	15408-1	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model
ČSN ISO/IEC	15408-2	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky
ČSN ISO/IEC	15408-3	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti
ČSN ISO/IEC	17799	Informační technologie - Soubor postupů pro řízení informační bezpečnosti
ČSN ISO	6166	Cenné papíry a příbuzné finanční nástroje - Mezinárodní systém identifikačního číslování cenných papírů (ISIN)
ČSN ISO	7775	Bankovnictví - Cenné papíry - Schéma pro typy zpráv
ČSN ISO	8372	Zpracování informací - Módy činnosti pro algoritmus 64-bitové blokové šifry
ČSN ISO	8730	Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu)
ČSN ISO	8731-1	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA
ČSN ISO	8731-2	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 2: Algoritmus autentikátora zprávy
ČSN ISO	8732	Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)
ČSN ISO	8908	Bankovnictví a souvisící finanční služby - Slovník a datové prvky
ČSN ISO	9564-1	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN

ČSN ISO	9564-2	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 2: Schválené algoritmy pro šifrování PIN
ČSN ISO	9735-5	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)
ČSN ISO	9735-6	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 6: Bezpečnostní autentizace a potvrzení (Zpráva AUTACK)
ČSN ISO/IEC	9796-2	Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy využívající hash funkci
ČSN ISO/IEC	9796-3	Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech
ČSN ISO/IEC	9797	Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry
ČSN ISO/IEC	9797-1	Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru
ČSN ISO/IEC	9798-1	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - 1. část: Obecný model
ČSN ISO/IEC	9798-2	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 2: Mechanismy používající symetrické šifrovací algoritmy
ČSN ISO/IEC	9798-3	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Autentizace entit používající algoritmus s veřejným klíčem
ČSN ISO/IEC	9798-4	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci
ČSN ISO/IEC	9798-5	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí
ČSN ISO	9807	Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu)
ČSN ISO/IEC	9979	Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů

C. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 10. Protokol CVP

Jaroslav Pinkava, PVT a.s.

1. Úvod

V minulém dílu byla podána informace o probíhající diskusi v rámci pracovní skupiny PKIX. Existují čtyři protokoly, které se problematikou ověřování (validation) certifikátů zabývají. Jsou to protokol OCSP, dále protokol SCVP (popsaný v minulém dílu), protokol v rámci DVCS a konečně protokol CVP (Certificate Validation Protocol). O tomto protokolu bude stávající díl.

Autorem protokolu je známý architekt bezpečnosti pan Denis Pinkas (firma Bull). První návrh protokolu vznikl v říjnu 2002, v lednu 2003 byl opublikován draft v druhé verzi.

2. Protokol CVP

Protokol lze použít pro následující účely:

1) dotaz směrovaný k politice ověřování či zjišťování informací, kterou podporuje CVP server;
2) ověření jednoho či více certifikátů veřejného klíče podle jedné z ověřovacích politik;
3) nalezení jedné či více certifikačních cest pro jeden či více certifikátů dle jedné politiky (k zjišťování informací).

Specifikace protokolu byly vytvářeny již tak, aby byly v souladu s požadavky na DPV a DPD dle [4], viz též [2]. Předpokládá se přitom, že mohou nastat všechny tři možné situace, tj. server může podporovat buď jen DPV či jen DPD anebo může podporovat obě možnosti.

Protokol umožňuje klientovi používat určité jednoduché předdefinované politiky (pro ověřování či zjišťování certifikačních informací) s několika málo proměnnými parametry. V zásadě se však předpokládá, že většina klientů se odkáže na ověřovací politiku používané aplikace anebo bude respektovat doporučovanou politiku serveru.

Server na příslušný dotaz musí vracet OID podporované politiky a může také vracet některé detaily předdefinovaných jednoduchých politik.

Ověřování certifikátů by vždy mělo probíhat na bázi určitých stanovených pravidel (politika ověřování). Pokud CVP server nepodporuje politiku požadovanou klientem, jeho odpovědí musí být chybové hlášení. A pokud klientský požadavek politiku nespecifikuje, odpověď serveru musí vyznačit, dle jaké politiky byla vytvořena.

Jestliže je ověření certifikátu vyžadováno v žádosti, pak tento certifikát musí být buď přímo součástí žádosti nebo žádost musí obsahovat jednoznačný odkaz na tento certifikát.

Server CVP musí mít ověřovaný certifikát k dispozici. Klient může svůj požadavek doplnit dalšími užitečnými certifikáty resp. revokační informací (odpovědi protokolu OCSP, CRL či delta CRL). Lze požadovat, aby server určil platnost certifikátu i v jiný časový

okamžik (jiný než stávající). CVP server musí získat revokační statut certifikátu pro čas obsažený v klientském požadavku. Není-li to možné, pak odpověď serveru je, že certifikát není platný (pro požadovaný časový okamžik).

Server CVP může k ověření platnosti certifikátu používat různé informační zdroje – podle politiky pro ověřovaní. Odpověď serveru CVP indikuje jednu z těchto tří možností:

- certifikát je platný ve smyslu příslušné politiky pro ověřování;
- certifikát není platný ve smyslu politiky pro ověřování;
- platnost certifikátu není známa (dle politiky pro ověřování).

Spolu s odpovědí, že certifikát není platný musí být uváděn i důvod této neplatnosti. Pokud je certifikát naopak platný, pak server v odpovědi musí obsáhnout i příslušná ověřovací data.

DPD (Delegated Path Discovery) by vždy měla být prováděna za platnosti určitých pravidel (politika zjišťování – discovery policy) a server musí reagovat obdobně jako při ověřování certifikátu (vracet chybové hlášení pokud nepodporuje klientem požadovanou politiku, označit v odpovědi, dle jaké politiky byla odpověď zpracována atd.). Odpověď serveru kromě obdoby tří výše popsaných možností může také obsahovat indikaci, že nebyla nalezena certifikační cesta (dle stávající politiky zjišťování).

Jestliže je to klientem požadováno, pak server může odpovědi pro DPV i DPD podepsat, přitom odpověď musí obsahovat přímý odkaz na certifikát serveru CVP – tím je odpověď autentizována. Stejně tak mohou být podepsány klientské požadavky (server CVP může požadovat autentizaci klienta). Při požadavku na důvěrnost (utajení) komunikace, je tato zajišťována bezpečnostním protokolem na nižší úrovni.

Draft dále specifikuje požadavky na politiky ověřování a zjišťování. Týž protokol lze použít jak pro iniciální (prvotní) ověření, tak i pro pozdější znovuověření.

3. K popisu CVP protokolu

Požadavek (DPV resp. DPD, může být eventuálně i podepsán) obsahuje následující data:

- verzi protokolu;
- nepovinné nonce (prevence znovuzasílání požadavků);
- buď identifikaci ověřovaného certifikátu či samotný certifikát a ke každému certifikátu dále (nepovinně) další užitečné certifikáty, revokační informace a jiné vhodné odkazy.
- politiku ověřovaní (zjišťování) – nepovinně;
- označení zda je to požadavek DPV či DPD a v návaznosti specifikace požadovaných odpovědí (např. zda má být přiložena časová značka atd.);
- nepovinně identifikaci strany zasílající požadavek a další data této strany;
- nepovinná rozšíření.

Po obdržení požadavku stanoví CVP zda

- zpráva má správný formát;
- odpovídající strana je nakonfigurována tak, že může poskytnout požadovanou službu;
- žádost obsahuje všechny potřebné informace.

Odpověď obsahuje následující data:

- verze protokolu;
- nepovinné Donce;
- tzv. major a minér status odpovědi;
- identifikaci certifikátu;
- odkaz na použitou politiku pro ověřování;
- druh požadované služby;
- čas odpovědi;
- časový moment pro který bylo ověřování provedeno;
- pořadové číslo odpovědi;
- cash všech parametrů odpovědi;
- identifikaci odpovídajícího serveru;
- odkaz na certifikát serveru;
- nepovinně identifikaci žádající strany a další jeho data;
- případně některé kontextuální informace;
- pole pro budoucí rozšíření.

V draftu je dále obsažena podrobná a okomentovaná syntaxe ASN.1 celého protokolu.

4. Další poznámky

Kromě popisu samotného protokolu obsahuje draft definice některých jednoduchých politik pro ověřování a zjišťování (podpora těchto politik je nepovinná).

V některých sítích (speciálně těch, které obsahují firewally) nemusí být CVP server schopný získat všechny informace, které potřebuje ke zpracování odpovědi. K tomuto účelu však může využít služeb jiných CVP serverů - čehož si klient nemusí být vědom. Draft obsahuje základní informace k vytváření komunikace mezi jednotlivými CVP servery.

V dokumentu není stanoven závazný typ přenosového protokolu, jsou však rozebrány následující možnosti: protokol TCP, HTTP a email.

5. Literatura

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

[2] předešlé díly tohoto seriálu

[3] Pinkas, D.: Certificate Validation Protocol
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-cvp-01.txt

[4] Pinkas, D.; Housley R.: Delegated Path Validation and Delegate path Discovery. Protocol requirements, http://www.ietf.cnri.reston.va.us/rfc/rfc3379.txt

D. Obecnost neznamená nejednoznačnost, aneb ještě malá poznámka k některým nedostatkům zákona o elektronickém podpisu před jeho novelizací

JUDr. Ján Matejka, Ústav státu a práva AV ČR

Příspěvek [1]polemizuje *s článkem P. Matese a V. Smejkala a jejich výkladem pojmu „orgán veřejné moci“ ve vztahu k ustanovení § 11 zákona o elektronickém podpisu před jeho novelizací zákonem 226/2002 Sb.*

ÚVOD

Článek kolegů Matese, P., a Smejkala, V., "Právní nebo technické normy" (BA 8/2002, s.61-63) se zřejmě snaží nastínit možné příčiny, resp. jednu z příčin, nestability našeho právního řádu, a to především se zřetelem k jeho přílišné kasuistice. Článek výše uvedených autorů je bezpochyby přínosem, pokud pojednává o obecných aspektech této problematiky, případně, a i to s výhradou, o některých aspektech elektronického podepisování či doktrinárním výkladu pojmu "orgán veřejné moci" [2] Dle našeho názoru jej však lze považovat za poněkud zavádějící v některých dalších aspektech. Pokusíme se vysvětlit proč.

JEŠTĚ K VÝKLADU § 11 ZÁKONA O ELEKTRONICKÉM PODPISU

Jak ostatně vyplývá z obsahu výše citovaného článku, jeho autoři kritizují (mnohdy jistě nevhodnou) kasuistiku našeho právního řádu, resp. jeho právních norem, přičemž se dožadují požadavku jejich obecnosti. Dle jejich názoru je totiž právní norma jakýmsi obecným pravidlem chování [3], avšak (jak dále uvádějí) náš právní řád jde prý v linii opačné a někdy se zdá, jakoby zákonodárce chtěl pamatovat na všechny možné detaily a varianty, takže obsah právních předpisů připomíná spíše technické normy, podrobně určující každý krok, který je třeba vykonat, čemuž pak odpovídá obsah i terminologie zákonů. Takovýto přístup, posílený nedostatečnou sebedůvěrou ve výklad obecně formulovaného předpisu, pak mnohdy, jak tvrdí výše uvedení autoři, způsobuje mimo jiné soustavné změny právního řadu. **Z toho pak výše uvedení autoři dovozují, že není třeba se dožadovat v případě jakékoli nejasnosti okamžité změny zákona, ale vhodnější je počkat si na výklad, který učiní praxe.**

Odhlédneme-li na okamžik od samotné právní (ne)závaznosti takovéhoto výkladu, klíčovou problematiku zde představuje ještě jedna otázka. Autoři totiž nesprávnost výše uvedeného přístupu demonstrují na příkladu výkladu ustanovení § 11 zákona o elektronickém podpisu, které považují, jak dle našeho soudu z článku vyplývá, právě za dostatečně obecné, jasné a tedy prosté jakékoliv potřeby jej novelizovat. V tomto ohledu výše uvedení autoři rovněž polemizují s některými již publikovanými právními názory [4] na tuto problematiku.

V těchto článcích mimo jiné také uvádíme [5], že zákon o elektronickém podpisu obsahuje, či dnes přesněji obsahoval [6], řadu právně nepříliš vyhovujících ustanoveních. Mimo jiné zde uvádíme (a v tom je příčina našeho sporu s výše uvedenými autory), že **§ 11 zákona o elektronickém podpisu je formulován dosti nejednoznačně a neostře**, což je vzhledem ke klíčové povinnosti, kterou zavádí, vskutku na povážení. Toto ustanovení (§ 11), byť obsahuje pouze jedinou větu, říká, že "v oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb". V tomto směru jsme v našem článku zastávali názor, že je zde použit velmi neostrý pojem "oblast" orgánů veřejné moci a může být tedy v některých případech sporné, zda je nutno používat tuto (jistě důvěryhodnou, avšak také nákladnou) formu podpisu i tam, kde s takovým orgánem pouze komunikuje soukromý subjekt - fyzická

osoba (např. v souvislosti s podáváním daňového přiznání). Uvedené jsme demonstrovali právě na zjevně neostré hranici pojmu "oblast", který lze jen sotva jednoznačně vyložit. Vycházeli jsme zde zejména z obvykle uváděného výkladového vodítka přirovnávajícímu "orgán veřejné moci" k "výkonu této moci" (nejde totiž o statický pojem) a nezbývalo nám než konstatovat, že komunikace soukromých subjektů s orgánem veřejné moci není výkonem ani oblastí výkonu této moci a že tedy **soukromá osoba podávající podání směrem k orgánu veřejné moci se patrně nemusí (ale může) podepisovat způsobem uvedeným v § 11**. Jinými slovy jsme neviděli důvod uvedené ustanovení (jde o kogentní veřejnoprávní normu) vykládat extensivně, tj. interpretovat uvedené ustanovení tak, aby se povinnost v této právní normě stanovená vztahovala i na fyzické či právnické osoby. Vzhledem k nejasnosti tohoto ustanovení, resp. tohoto pojmu jsme tedy doporučovali upřesnění uvedené formulace, případně vypuštění celého ustanovení, a to i z celé řady dalších důvodů (jako např. jeho neslučitelnost s právem ES, apod.). [7]

Autoři výše uvedeného článku však argumentují zjevně opačně, a to mimo jiné i tím, že podle jejich názoru je třeba chápat pojem "**oblast orgánů veřejné moci**" nikoli "jednosměrně" zejména z toho důvodu, že pokud by zákonodárce chtěl tento smysl ustanovení § 11 dát, pak by tak nepochybně i výslovně učinil. Dle našeho názoru však v tomto případě nejde o argumentaci relevantní, a to zejména vzhledem k veřejnoprávní povaze tohoto ustanovení, kde by naopak zákonodárce měl výslovně stanovit, že se toto ustanovení na tzv. "jednosměrnou" komunikaci vztahuje. [8]

V podobném duchu je ze strany autorů dále argumentováno, že pouze zaručený elektronický podpis ve smyslu § 2 písm. b) zákona o elektronickém podpisu zaručuje potřebnou vysoce jistou verifikaci osoby i obsahu úkonu, který činí, a že tedy není možno dospět k jinému závěru, než že právě ten má na mysli § 11 zákona, a to i v případě, že soukromý subjekt činí podání k orgánu veřejné moci. K tomuto argumentu je však třeba dodat zejména to, že samotný zaručený elektronický podpis (bez kvalifikovaného certifikátu, apod.) toho v tomto ohledu příliš mnoho nezaručuje - a vypovídací hodnota takového podpisu nemusí, ale může být zcela srovnatelná (snad vyjma požadavku integrity) s běžným elektronickým podpisem (např. údajem o odesílateli SMS zprávy, označením odesílatele e mailu, apod.). Navíc v tradiční papírové a co do podpisu vlastnoruční podobě také nikde nenalezneme obdobu požadavku vysoce jisté verifikaci osoby i obsahu úkonu, tak jak uvádějí oba autoři. V tomto ohledu tento argument považujeme tedy za zavádějící.

Ať již má však pravdu kdokoliv, je třeba zdůraznit, že **spory ohledně § 11 navíc provází tento zákon již od jeho počátku**. V žádném z předložených návrhů tohoto zákona se povinnost podobné té v § 11 nevyskytovala a do samotného textu zákona se toto ustanovení dostalo mezi jeho druhým a třetím čtením jako důsledek přijatého pozměňovacího návrhu. Důvodová zpráva k tomuto zákonu je tedy pochopitelně nepoužitelná. Pár měsíců po nabytí účinnosti tohoto zákona se nad výkladem ustanovení § 11 začalo diskutovat, zřídkakdy však s jednoznačným výsledkem.

Schůzek, konferencí a různých porad, které se rozsahem (extenzí) § 11 zabývaly bylo v tomto ohledu rovněž nepočítaně [9], a publikovaných názorů, vzhledem k pozornosti, které elektronický podpis v odborné literatuře získal, pak také. V zásadě zde však šlo pouze o názor na předmětnou problematiku, resp. na nejasnost výkladu § 11. Prvním významným činem (a rovněž medializovaným) či spíše klíčovým příspěvkem z řad kritiků tohoto zákona byla reakce Ministerstva práce a sociálních věcí (MPSV), které právě z důvodů nejasnosti § 11 tohoto zákona zastavilo zásadní projekt zavádění elektronického podpisu do státní správy. Zastavení tohoto projektu bylo ze strany MPSV rovněž několikráte zdůvodňováno [10]. **Této nepříliš jasné situace si zjevně povšimla také vláda České republiky**, která dne 9. ledna 2002 přijala usnesení č. 20 k Zelené knize o elektronickém obchodu, jehož obsahem byl mimo jiné i její závazek novelizací konkretizovat §11 zákona o elektronickém podpisu [11].

Dle našeho názoru lze tedy sotva souhlasit s autory výše citovaného článku, že výklad tohoto ustanovení je (a vždy byl) jasný a že tedy nebylo třeba se dožadovat případné změny zákona a precizovat tak (dosud spornou) extenzi tohoto ustanovení.

VÝZNAM JASNÉ A JEDNOZNAČNÉ FORMULACE V PRÁVNÍM ŘÁDU

Je nepochybně pravdou, a v tom lze s autory výše citovaného článku jistě souhlasit, že právní normy, a to zejména ty zákonné, mají být obecné. Je však třeba poznamenat, a tomu se autoři ve svém textu k jejich škodě nevěnovali, že **obecnost v tomto smyslu nesmí znamenat vágnost a nejednoznačnost právní normy**, ať již jako celku, nebo její části.
K tomu, abychom mohli určitou normu považovat za normu právní, je třeba, aby její závaznost byla obecná, a to včetně předmětu její úpravy. Obecností co do předmětu se v tomto ohledu rozumí zejména to, že právní norma obecně vymezuje svou skutkovou podstatu (např. tak, že stanoví povinnost používat určitý typ elektronického podpisu), tj. že nikdy nemůže řešit určitý konkrétní případ. Tato stránka obecnosti právní normy je ale celkem nepochybná.

O poznání složitější je však otázka obecnosti právní normy co do jejích adresátů (subjektů právní normy) a o tu v tomto případě také jde. Z požadavku obecnosti právní normy co do jejích subjektů (adresátů) však zároveň vyplývá, že nemůže být adresována jmenovitě toliko určité osobě (např. konkrétnímu pracovníkovi, koncipientovi či advokátovi), **obecnost právní normy tedy nespočívá pouze v předmětu její úpravy, ale též ve způsobu určení jejich adresátů**. Adresát právní normy tedy musí být určen a vymezen určitými obecnými znaky, resp. množinou těchto znaků. Obecnost právní normy v tomto smyslu (tedy co do jejích subjektů - adresátů) je pak dána tehdy, jestliže jejím subjektem jsou všechny subjekty práv, které jsou prvkem dané množiny. Dalším nezbytným, byť navýsost souvisejícím a potřebným, požadavkem je pak **srozumitelnost, tj. jasnost a jednoznačnost** formulace právní normy. Právní norma je totiž dále studována, vykládána a ve svém důsledku pak zejména aplikována v každodenní praxi (ať již úřední, soudní, advokátní či jiné). V zásadě jakýkoliv, byť sebemenší, formulační nedostatek právní normy pak má za následek, že se jím tato praxe zatěžuje, vyvolává četné spory o výklad, zbytečné polemiky a porady o skutečném obsahu právního předpisu či jeho jednotlivých právních norem. [12]

Pokud zákonodárce formuluje právní normu tak, že její předmět co do subjektů (adresátů) váže na právně značně nejednoznačný a nejasný pojem "oblast", tak lze skutečně jen hádat (resp.ji složitě vykládat) a polemizovat nad jejím skutečným obsahem. Vyjma výše uvedených problémů, pak takový přístup zbytečně nabourává tolik nezbytný požadavek právní jistoty.

SOULAD § 11 S PRÁVEM EVROPSKÝCH SPOLEČENSTVÍ

Jedním z dalších, dle našeho soudu nesprávných, závěrů obou výše uvedených autorů je tvrzení, že ustanovení § 11 tohoto zákona je zcela v souladu s příslušnou směrnicí ES, resp. s jejím čl. 3 odst. 7, které, jak uvádějí autoři v poznámce pod čarou, údajně dovoluje členským státům podmínit používání elektronického podpisu ve veřejném sektoru případnými doplňujícími podmínkami. Čl. 3 odst. 7 této směrnice vskutku obdobné ustanovení obsahuje, avšak zároveň, a to v tomtéž článku, dále uvádí, že "…Tyto podmínky musí být objektivní, transparentní, úměrné a prosté diskriminace a smí se vztahovat výlučně na specifické charakteristiky daného použití. Tyto podmínky však nesmějí pro občany vytvářet překážky pro využívání služeb přesahující hranice či přeshraniční služby." [13] Při dočtení uvedeného článku do konce je tedy zjevné, že tyto podmínky nesmí být překážkou pro služby

poskytované občanům "přes hranice". Hlavní zákonnou podmínkou pro užívání elektronického podpisu ve veřejném sektoru je však v případě ČR (alespoň pokud dáme autorům při jejich výkladu §11 zapravdu), ta skutečnost, že musí jít o **zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb** (§ 11). Z toho, že zákon o elektronickém podpisu (§ 10 odst. 5) umožňuje udělit akreditaci jen takovému poskytovateli certifikačních služeb, který má sídlo na území ČR, lze dovodit, že se zde akreditace tedy uděluje toliko na základě územního principu, což je v rozporu se zakládajícími smlouvami ES, konkrétně pak s volným pohybem služeb [14].

Zákon o elektronickém podpisu byl v minulosti rovněž předmětem řady expertíz a stanovisek, kde byla vyslovena jeho zjevná nekompatibilita s právem ES, a to i výslovně vůči ustanovení § 11 tohoto zákona [15]. Zákon tak zůstává, bohužel v celé řadě dalších ustanovení (v rozporu s tvrzením v důvodové zprávě [16]) **neslučitelný s právem Evropských společenství** (zejména pak ustanovení § 2, §10, § 11 a § 16).

MÍSTO ZÁVĚRU, ANEB § 11 ZÁKONA BYL NOVELIZOVÁN

S účinností od 1.7.2002 byl přijat zákon č. 226/2000 Sb., kterým se vyjma klíčových procesních norem, na které se v některých otázkách při přijetí zákona o elektronickém podpisu jaksi pozapomnělo (trestní řád, správní řád, zákon o správě daní a poplatků) mění a doplňuje také § 11 zákona o elektronickém podpisu. Pátá část této novely tak doplňuje a konkretizuje extenzi dosud problematického §11 zákona o elektronickém podpisu, kde se za dosud existující ustanovení tohoto paragrafu doplňuje text "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.". Zde zákonodárce svým způsobem odstraňuje řadu nejasností spočívajících v dosavadní celkové neurčitosti a zavádí tak tzv. jednoznačný identifikátor (tedy údaj uvedený na certifikátu), který se ukázal jako nezbytný pro potřeby praxe. Jedním z důsledků této poslední novely zákona o elektronickém podpisu je také to, že pro komunikaci s orgánem veřejné moci nelze používat anonymní certifikát V souvislosti s touto novelou pak také Ministerstvo práce a sociálních věcí zahájilo projekt podávání žádostí o dávky sociální podpory elektronickou cestou. Jako součást kvalifikovaného certifikátu tak MPSV (zcela v souladu s touto novelou) vyžaduje identifikátor klienta MPSV. Tento identifikátor si musí nechat podepisující se osoba zapsat do svého kvalifikovaného certifikátu při jeho vystavení. **Tato novela (dále jen novela) reflektuje většinu požadavků jak praxe [18], tak i právní teorie** [18]. K těmto krokům se, jak již bylo výše uvedeno, rovněž nedávno zavázala i vláda. [19]

Jak vyplývá z výše uvedeného, nedomníváme se tedy, že nebylo třeba se dožadovat novelizace § 11 zákona o elektronickém podpisu ve smyslu upřesnění jeho extenze. **Dle našeho názoru skutečně nelze zjevné nedostatky právního řádu odstraňovat pouhým výkladem**. Opačný přístup by nejenom nabourával požadavek právní jistoty, ale zejména by v obdobných případech vytvářel řadu dalších překážek v již poměrně komplikované problematice e-government.

V posledních letech bohužel dochází stále častěji k vytváření aplikačně velmi problematických zákonů, kde se pak stává téměř běžné, že se nepostupuje podle zákona, ale pouze podle výkladu tohoto zákona [20]. Vyjma samotného zákona o elektronickém podpisu, jehož § 11 byl předmětem tohoto diskusního příspěvku, lze řadu dalších nikoli nevýznamných nedostatků spatřovat zejména v zákoně č. 101/2000 Sb. ČR o ochraně osobních údajů, kde lze zcela souhlasit s názorem [21], že se **v současné době opravdu vzhledem k obdobně nejasným formulacím nepostupuje podle zákona, ale podle výkladu tohoto zákona**

správním úřadem. Naštěstí se některé nedostatky daří odstranit brzkou novelizací [22], jiné (mnohdy i zásadnější) otázky však nadále přetrvávají [23]. Lze jen doufat, že se naše legislativa nebude ubírat podobným směrem častěji.

Poznámky

[1] Tento diskusní příspěvek byl zpracován na základě grantu uděleného GA AV ČR, registrační číslo B7068203

[2] Co se týče výkladu tohoto pojmu, jsme (a byli jsme) s výše uvedenými názory jednotní.

[3] V tomto ohledu se však, patrně vědomě, dopouštějí nikoli nepodstatného zjednodušení. Právní normy jistě mohou být vymezeny z různých aspektů a k jejich definici lze tudíž přistupovat různým způsobem. Převládají definice, které chápou právní normy jako určitým způsobem kvalifikovaná pravidla lidského chování, stejně tak ale existují i jiné. Obecnost se však k pojmu právní normy per definicionem váže zejména ve smyslu její závaznosti. I kasuistická (nikoli tedy obecná) právní norma, pokud je obecně závazná, je nepochybně normou právní.

[4] Zejména pak s našimi kritickými poznámkami k zákonu o elektronickém podpisu uvedenými v článku K právní úpravě elektronického podpisu, Bulletin Advokacie, 3/2002, s. 27-41 a dále pak s článkem Matejka, J., Úprava elektronického podpisu v právním řádu ČR, Právník, č.6, 2001, s. 557 - 586

[5] Matejka, J., Chum, V., K právní úpravě elektronického podpisu, Bulletin Advokacie, 3/2002, s.39-41

[6] Zákon o elektronickém podpisu byl s účinností od 1.7.2002 v tomto ohledu novelizován (k tomu více v závěru tohoto článku).

[7] K tomu více Matejka, J., Úprava elektronického podpisu v právním řádu ČR, Právník, č.6, 2001, s. 580 a násl.

[8] Viz čl.2 odst.3 čl. 4 odst.1 Listiny základních práv a svobod

[9] Jako zřejmě nejvýznamnější zde uvádím zejména akce Sdružení pro informační společnost (SPIS), a to zejména diskusní setkání ředitelů odborů informatiky ministerstev a dalších orgánů statní správy na téma implementace elektronického podpisu do státní správy Kaiserštejnský palác (dne 13.2.2002), dále pak Tuchlovice (patrně ve dne 25.5.2001) a další. Tato problematika však byla předmětem řady porad a jednání v rámci Úřadu pro ochranu osobních údajů.

[10] Např. Kučera, R., MPSV: elektronický podpis nebude?!, 11.12.2001, zive.cz

[11] Toto usnesení vlády, resp. jeho příloha č.2 (Návrh analýzy právních předpisů) v tomto ohledu výslovně konstatuje, že § 11 zákona o elektronickém podpisu je výkladově problematický, v tomto ohledu pak také stanoví související závazky.

[12] K tomu více Knapp, V., Tvorba práva a její současné problémy, Linde Praha a.s., 1998, s.34 a násl.

[13] Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

[14] Požadavek v § 10 odst. 5, že akreditovaný poskytovatel certifikačních služeb musí mít sídlo na území ČR, je v rozporu s čl. 3 odst. 2 a čl. 4 odst. 1 věta druhá směrnice.

[15] Např. stanovisko Odboru kompatibility s právem ES Úřadu vlády ze dne 23. 8. 2001, kde byla tímto odborem jasně stanovena neslučitelnost zákona o elektronickém podpisu s právem ES (prováděcí vyhláška k tomuto zákonu však byla shledána zcela slučitelnou), další expertíza (se stejným výsledkem) pak byla provedena Parlamentním institutem.

[16] Viz Část E důvodové zprávy

[17] Faltýnek, M., Zákon o elektronickém podpisu v daňové správě, Daně, 1/2001, s.12

[18] Např. Matejka, J., Vybrané první překážky elektronického obchodu, Parlamentní zpravodaj, 3/2002, s.12 - 13

[19] Viz dokument Zelená kniha o elektronickém obchodu, který vláda přijala na svém zasedání ze dne 9.1.2002

[20] Není pochyb, že problémů, které takovýto přístup pak přináší je celá řada, jejich komplexní zpracování by nedalo ne na článek, ale na samostatnou monografii.

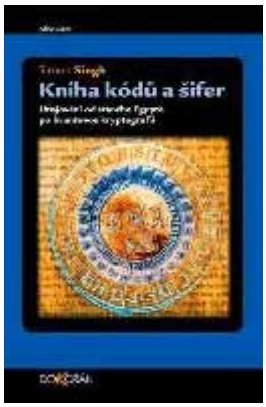
[21] Píchová, I., K ochraně osobních údajů v pracovněprávních vztazích, Právo a zaměstnání č.12/2001, s.5-7

[22] K původně sporným otázkám osobní i věcné působnosti zákona o ochraně osobních údajů srovnej např. argumentaci Sokol, T., Zákon o ochraně osobních údajů se na advokáta nevztahuje, BA 92000 . Většinu těchto otázek se již podařilo odstranit novelizací, některé další však bohužel přetrvávají

[23] K absurdním (a výkladově nepochybně možným) důsledkům zákona o ochraně osobních údajů více Kindl, M., K "novátorským" důsledkům zákona o ochraně osobních údajů, Právní rozhledy, č.2, 2001

E. Letem šifrovým světem

Knižní novinka



Simon Singh : Kniha kódů a šifer. Utajování od starého Egypta po kvantovou kryptografii. Překlad *Petr Koubský*, odborná revize *Vlastimil Klíma*, asi 400 stran, 180 ilustrací, tabulek a příloh, cca 350 Kč, ISBN 80-86569-18-7, řada Aliter. Singhova kniha mapuje historii šifrování i současný stav kryptologie a podrobně zpracovává klíčová a nejzajímavější témata. Díky přístupnému stylu a jasnému vysvětlení řady složitých šifrovacích systémů a algoritmů lze knihu doporučit každému zájemci o tuto nesporně zajímavou oblast lidské činnosti.
http://www.dokoran.cz/ep2003/sifry.html

Crypto-World na CD CHIPU 4/03

Koncem března (27.3.03) vyjde CD příloha časopisu CHIP 4/03 s tématickým obsahem "Bezpečnost dat". V rámci tohoto tématu budou k dispozici příspěvky k tématům ochrana a obnova dat, antiviry, firewally, šifrování, internetová bezpečnost...

Na CD proto najdete i statickou verzi domácí stránky Crypto-Worldu http://www.mujweb.cz/veda/gcucmp/ (http://www.crypro-world.tk). Vzhledem k omezenému prostoru, který mi byl přidělen, zde naleznete pouze kompletní ročník 2002 a prvé dva e-ziny z roku 2003. Dále zde najdete kompletní informace o soutěži v luštění, která probíhala v roce 2000 a 2001 a obsahy všech dosud vyšlých čísel Crypto-Worldu (1999-2003).

MFF UK Praha

Informace k přednášce **Úvod do klasických a moderních metod šifrování** ALG082, včetně doprovodných přednáškových textů naleznete na
http://adela.karlin.mff.cuni.cz/~tuma/ciphers.html

Cryptome byl hacknut!

Jeden z nejznámějších serverů v oblasti informací s bezpečnostní a kryptografickou tématikou – Cryptome (http://cryptome.org) byl 26. února 2003 napaden hackery. Útok byl „úspěšný“ a celý obsah serveru byl kompletně vymazán. K útoku se přihlásil bighawk (bighawk@kryptology.org) ze skupiny "Phrack High Counsil". Blíže se dočtete na stránkách jak postižených http://cryptome.org/cryptome-hack.htm, http://cryptome.org/cryptome-hack2.htm , tak na hackerské stránce http://phrack.efnet.ru/ (heslo cryptome).

AEC TrustPort CA

Na stránkách certifikační autority AEC TrustPort CA byla dána do provozu AEC TrustPort TimeStamp Authority (AEC TP TSA) - první autorita časové značky u nás. Slouží k vydávání tzv. časových razítek, s jejichž pomocí lze pro elektronické transakce, formuláře, archivovaná data, elektronický podpis apod. zajistit jejich přesné určení v čase. Toto řešení si můžete bezplatně vyzkoušet pomocí aplikace TS Client, která je k dispozici ke stažení na stránkách http://www.trustport.cz . Na této stránce je také dostupná politika autority časových značek http://www.trustport.cz/pub/TSA_policy.pdf .

Chyba v SendMailu

Poštovní agent Sendmail obsahuje vážnou bezpečnostní díru! Vzhledem k tomu, že velká většina světového e-mailového provozu prochází právě přes tento „open source" software, je tato zpráva zvláště závažná.

Uvedená chyba se týká Sendmailu ve verzích 5.79 až 8.12.7. Jedná se o tzv. „buffer overrun exploit" chybu velice podobnou chybě v Microsoft SQL serveru, kterou nedávno zneužil internetový červ Slammer. Zneužitím uvedené díry mohou případní hackeři dostat sendmailový server zcela pod svoji kontrolu. Přitom k tomu není třeba na serveru spouštět žádný soubor, ale stačí na něj zaslat speciálně upravený e-mail. Výsledkem takového útoku pak může být v lepším případě zpomalení činnosti serveru a v horším kompromitace veškeré příchozí a odchozí komunikace. Sendmail Consortium doporučuje správcům uvedených verzí Sendmailu, aby provedli upgrade na verzi 8.12.8 nebo bezpečnostní díru ošetřili pomocí bezpečnostního patche. Upgrade i patch jsou dostupné na http://www.sendmail.org.

VI. ročník konference ISSS 2003 (Internet ve státní správě a samosprávě)

Konference se bude konat v kongresovém centru Aldis, v Hradci Králové ve dnech 24. - 25. 3. 2003. (http://www.isss.cz)

Výběr z hlavních témat ISSS 2003:

- Role nového ministerstva IT v rozvoji informatizace veřejné správy
- E-government
- Komunikační infrastruktura IS veřejné správy
- Otázky bezpečnosti informačních systémů
- Geografické informační systémy pro státní správu a samosprávu
- Problematika informatizace krajských úřadů a obcí s rozšířenou působností
- Seminář o webech měst a obcí

Podrobný program konference naleznete zde: http://www.isss.cz/servis.asp

Konference Security 2003

Stejně jako v minulých letech se i letos stane pražský Národní dům na Vinohradech na jeden den útočištěm příznivců bezpečnosti informačních a komunikačních technologií.

Pořádající společnost AEC Data Security Company srdečně zve všechny zájemce o aktuální informace ze světa antivirové ochrany a informační bezpečnosti na konferenci Security 2003, která se bude konat v úterý 15. dubna 2003 již tradičně v reprezentativních prostorách Národního domu na Vinohradech v Praze. Záštitu nad konferencí převzalo Ministerstvo vnitra České republiky

Stejně jako každý rok je program rozdělen do několika bloků. První blok nazvaný „Bezpečnost dat“ bude věnován obecným i praktickým otázkám informační bezpečnosti jako takové. Součástí bude přednáška zabývající se certifikační autoritou ve spojení s praktickou aplikací časových značek. Druhý programový blok je do značné míry novinkou. Je jím vystoupení zástupců zahraničních společností, které se na pořádání konference taktéž podílí. Účastníci Security 2003 si budou moci vyslechnout dvě přednášky na téma antivirové problematiky. První přednese antivirový specialista finské společnosti F-Secure Corporation - Mikko Hypponen a druhou zástupce maďarské společnosti Virus Buster – Tibor Bial. Třetí závěrečný přednáškový blok konference bude tradičně patřit počítačovým virům a ochraně proti nim.

Přihlásit k účasti se můžete pomocí on-line formuláře, který najdete na adrese https://www.aec.cz/forms/formsecurity.asp , nebo e-mailem na adrese konference@aec.cz . Další podrobnosti najdete na www.security2003.cz .

BIFNS 2003 - Bezpečnost informácií vo finančnom a nefinančnom sektore

6. stretnutie bezpečnostných managerov vo Vysokých Tatrach
sa uskutoční v dňoch 15.-17.10.2003 v rámci tradičnej medzinárodnej odbornej konferencie

Vybrané diskúsne okruhy a otázky:
- Ochrana osobných údajov a informácií o klientoch a zákazníkoch
- Bezpečnostná politika a stratégia
- Metodológia riadenia bezpečnosti
- Analýza a management bezpečnostných rizík
- Bezpečnostný audit
- Prienik do informačného systému
- Únik doverných informácií
- Havarijné plánovanie a plány obnovy

Bližšie informácie o podujatí získate u organizátora konferencie – spoločnosti New Management Conferences - NMC s.r.o. Žilina

Richard Vanovčan (NMC spol. s r.o.)
Pittsburská 4, P.O.BOX 39, 010 08 Žilina, Slovakia
e-mail: nmc@internet.sk web: http://www.nmc.sk
tel: 00421-41-5166661, 5655229
fax: 00421-41-5655 229

O čem jsme psali v březnu 2000 - 2002

Crypto-World 3/2000

Crypto-World 3/2001

Crypto-World 3/2002

F. 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 neprocházejí 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.crypto-world.tk (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
pavel.vondruska@ct.cz
vondruska.p@seznam.cz
pavel.vondruska@post.cz