Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 7-8/2001 1. srpen 2001

7-8/2001

Připravil : Mgr.Pavel Vondruška,

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>300 e-mail výtisků)

OBSAH : **Str.**

A. Malé ohlédnutí za dalším rokem Crypto-Worldu (P.Vondruška) 2- 5
B. Standardizační proces v oblasti elektronického podpisu v EU a ČR (D.Bosáková, P.Vondruška) 6-13
C. XML signature (J.Klimeš) 14-18
D. O základním výzkumu v HP laboratořích v Bristolu, průmyslovém rozvoji a ekonomickém růstu (J. Hrubý) 19-21
E. Letem šifrovým světem 22-27
1. Skljarov (ElcomSoft) zatčen za šíření demoverze programu ke čtení zabezpečených elektronických knih ! (P.Vondruška) 22
2. FIPS PUB 140-2, bezpečnostní požadavky na kryptografické moduly (J.Pinkava) 23-24
3. Faktorizace velkých čísel - nová podoba výzvy RSA (J.Pinkava) 24-25
4. –7. Další krátké informace 26-27
F. Závěrečné informace 28

Příloha : priloha78.zip
(dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

A. Malé ohlédnutí za dalším rokem Crypto-Worldu

Mgr. Pavel Vondruška (ÚOOÚ)

Vážení čtenáři,

uběhl další rok vydávání našeho e-zinu (sešitu, který je vydáván a rozesílán v elektronické podobě). Prvé číslo sešitu vzniklo a bylo rozesláno v září roku 1999. Předcházelo mu nepravidelné rozesílání informací a upozornění na zajímavé články, které souvisely s kryptologií. Sešit sloužil původně velmi úzké skupině lidí – členů kryptologické sekce Jednoty českých matematiků a fyziků. Postupně byl rozesílán dalším zájemcům. Do září roku 2000 jsem na přípravě sešitu pracoval sám. Na podzim roku 2000 se přidal k přípravě ing.Jaroslav Pinkava. Jeho zásluhou je otiskován rozsáhlý seriál „Kryptografie a normy“. Tento seriál může sloužit jako velice slušný podklad k základní orientaci v dané problematice. Z ohlasů vím, že si jej řada studentů skutečně za tímto účelem uschovává a používá. Některé články k elektronickému podpisu byly zase použity jako podklad pro bakalářské a diplomové práce jiných našich čtenářů. Postupně se začal zvyšovat počet našich odběratelů. Všechny práce spojené s přípravou časopisu byly dělány zcela zdarma, články nejsou placené. Na základě jednání s některými firmami je možné, že získáme sponzorský dar, který nám umožní v několika příštích měsících za poskytnutí článku k otištění platit symbolickou částku. Forma sponzorského daru je nejvhodnější způsob, jak si udržet nezávislost na komerčních zájmech a současně pokrýt náklady vzniklé s přípravou časopisu a symbolicky odměnit lidi okolo Crypto-Worldu za čas, který časopisu věnují. Sponzorský dar není (a z jeho definice nemůže) být spojen s žádnou protislužbou, reklamou apod. Myslíme si však, že čtenáři mají právo vědět, kdo peníze na odměny věnoval, a tak každého, kdo některé z čísel bude sponzorovat, uvedeme na vhodném místě - např. na titulní straně (?, logo a plný název firmy). Tuto informaci můžete současně chápat i jako výzvu pro vaši firmu. Pokud získáme více prostředků, budeme samozřejmě zpětně schopni poskytnout více článků od více autorů.

Statistika rozvoje Crypto-Worldu

1999

	9/99	10/99	11/99	12/99
Odběratelů	25	31	35	47
Stran	7	10	9	9
Bytů	118 655	163 382	312 601	370 720

2000

	1/2000	2/2000	3/2000	4/2000	5/2000	6/2000
Odběratelů	62	76	90	102	107	116
Stran	9	11	11	13	15	16
Bytů	208 173	215 768	212 279	333 340	354 749	502 347

	7-8/2000	9/2000	10/2000	11/2000	12/2000	V/2000
Odběratelů	163	190	200	228	230	230
Stran	19	20	24	19	21	17
Bytů	150 000	188 227	284 108	254 586	146 382	291 528

2001

	1/2001	2/2001	3/2001	4/2001	5/2001	6/2001	7-8/2001
Odběratelů	240	250	260	270	280	300	308
Stran	22	29	23	25	19	28	28
Bytů	166 242	231 824	206 663	304 903	391 948	1 084 637	550 000(?)

Při rozeslání posledního čísla našeho e-zinu jsme vám předložili malou anketu. Anketa měla dát odpověď na otázku, zda je mezi čtenáři zájem o obdobnou soutěž jako v loňském roce. Další otázky se týkaly zřízení nové rubriky a distribuce e-zinu. Celkem jsme na položené otázky dostali odpovědi od 17-ti odběratelů.

Otázky, které jsme Vám položili, zněly:
f) od minulého čísla jsme začali zveřejňovat i články s právním obsahem, které mají vztah k tématům, které jsou v Crypto-Worldu uváděny, máte zájem i o takové články ?
g) v loňském roce probíhala soutěž v luštění základních kryptografických systémů, do soutěže se z počátku zapojilo 30 lidí, ale řada z nich úkoly nedořešila s odůvodněním, že jsou příliš těžké. Máte zájem o podobnou - lehčí - soutěž i v tomto roce ?
h) v případě, že by probíhala soutěž i na podzim tohoto roku - zúčastnil byste se ?
i) v případě, že by probíhala soutěž i na podzim tohoto roku - mohl byste / vaše firma věnovat nějakou zajímavou cenu pro vítěze ?
j) vadilo by vám, kdyby se objevila další rubrika - za Letem šifrovým světem - ve které by byly představovány firmy (pouze české), které se zabývají informační bezpečností, rozsah 1 strana ? Obsahem bude krátká historie firmy, přehled služeb a produktů a spojení na tuto firmu. V každém čísle by byla představena 1 firma. Nebudete to považovat za nevhodné ?
k) dostáváte Crypto-World pravidelně?
l) máte problémy s otevřením příloh, jeho tiskem apod. ?
m) není moc velký ?, moc malý ?
n) je stránka http://www.mujweb.cz/veda/gcucmp často nedostupná, špatně přístupná ?
Pro úplnost dodám, že body a) až e) nebyly otázky, ale různé informace

Výsledky:

	f	g	h	i	j	k	l	m	n
1	A	-	N	A	N	A	1x	OK	OK
2	N	A	N	M	N	A	N	OK	-
3	A	-	A	N	A	A	4	OK	OK
4	A	A	A	N	N	A	N	OK	OK
5	A	-	-	N	N	A	N	OK	-
6	N	A	A	N	N	A	N	OK	-
7	A	A	A	A	N	A	N	OK	OK
8	A	A	A	N	N	A	N	OK	OK
9	A	A	A	A	A	A	1x	Malý	OK
10	A	N	N	N	A	A	N	OK	OK
11	A	A	A	N	N	A	N	OK	OK
12	A	A	A	M	N	A	N	OK	OK
13	A	A	A	N	N	A	N	OK	OK
14	A	A	A	A	N	A	N	OK	OK
15	A	A	N	A	N	A	N	OK	OK
16	A	A	A	N	N	A	N	OK	OK
17	A	A	A	N	A	A	N	OK	OK
	A	***A***	***A***	**-**	***N***	***A***	***N***	***OK***	***OK***

Legenda
A : ano N : ne
M : možná - : nezodpovězeno

Mile nás překvapila ochota firem věnovat ceny do soutěže (děkujeme). Mimo již "tradiční ceny" (certifikáty k datům pro vytváření elektronického podpisu) jsme získali i velice zajímavou nabídku loňského účastníka soutěže - čtenáře z Bulharska. Zde je jeho nabídka:
"MOHU NABIDNOUT BEDNU ZNACKOVEHO, OPRAVDU KVALITNIHO BULHARSKEHO VINA ".

Tím se dostáváme k nově připravované soutěži. Tentokráte bude na přání řady účastníků soutěže o něco lehčí a bude se opět skládat z úkolů, které prověří schopnosti soutěžících ze schopnosti řešit lehké úkoly z oblasti kryptologie. Proběhne opět v období září - prosinec. V minulé soutěži jsme probrali podrobně steganografii, jednoduchou záměnu, transpozici a složitou záměnu (periodické heslo). Nyní navážeme kódovou knihou a potom úkoly z modernější kryptografie. Připravuji opravdovou lahůdku - čtenáři se na závěr soutěže mohou pokusit rozšifrovat text zašifrovaný bezpečnou šifrou RSA (trochu samozřejmě napovím ....). Přeji hodně úspěchů.

Na závěr ještě několik přehledů a statistik:

Články, které vás nejvíce zaujaly (dle kladných reakcí):

1. Soutěž (9/2000-12/2000)
2. Seriál článků o prvočíslech (4/2000-78/2000)
3. Seriál článků „Kryptografie a normy“ (9/2000-6/2001)
4. Seriál článků „Codetalkers“ (4/2000-6/2000)

Odkud jsou naši čtenáři :

Česká republika, Slovenská republika, Spolková republika Německo, USA, Rakousko, Belgie, Bulharsko, Polsko

Statistika přístupů na stránku Crypto-Worldu za období 11.srpen 2000-27. červenec 2001

Datum registrace 11. srpen 2000

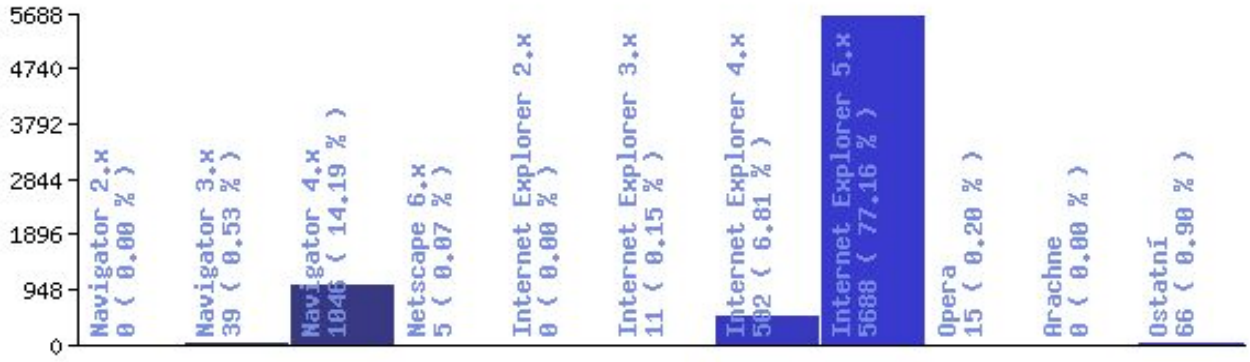
Celkový počet přístupů	**7375**
Průměrný denní počet přístupů	**21.01**
Průměrný počet přístupů za hodinu	**0.88**
Datum a čas posledního přístupu	**27. červenec 2001 21:25:17**

Nejúspěšnější den těchto stránek byl	**12. září 2000** se **188 přístupy**
Nejúspěšnější měsíc těchto stránek byl	**říjen 2000** s **1071** přístupy
Nejúspěšnější rok těchto stránek byl	**2000** s **3964** přístupy

Mezi 0:00 a 3:59	**178**	přístupů	(**2.41 %** všech přístupů)
Mezi 4:00 a 7:59	**458**	přístupů	(**6.21 %** všech přístupů)
Mezi 8:00 a 11:59	**2188**	přístupů	(**29.67 %** všech přístupů)
Mezi 12:00 a 15:59	**2321**	přístupů	(**31.47 %** všech přístupů)
Mezi 16:00 a 19:59	**1261**	přístupů	(**17.10 %** všech přístupů)
Mezi 20:00 a 23:59	**965**	přístupů	(**13.08 %** všech přístupů)

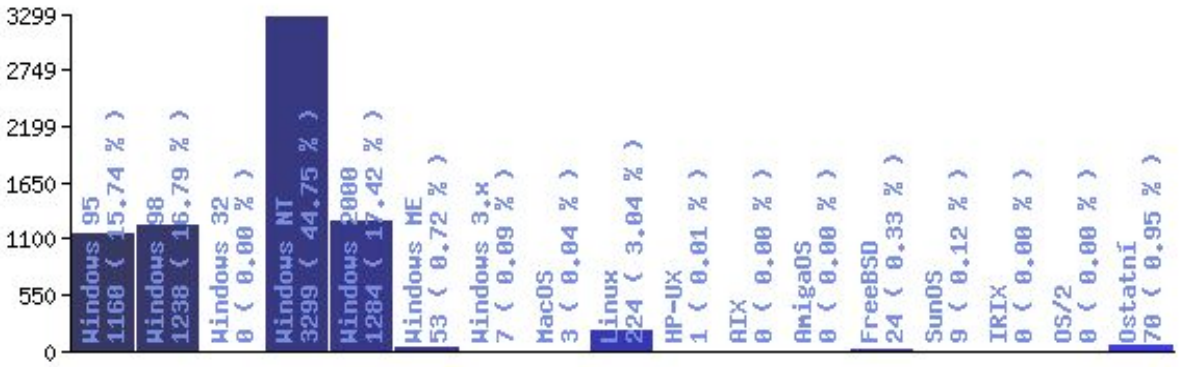
Pondělky	**1479** přístupů (**20.05%** všech přístupů)	Průměrně **29.57** přístupů
Úterky	**1360** přístupů (**18.44%** všech přístupů)	Průměrně **27.19** přístupů
Středy	**1444** přístupů (**19.58%** všech přístupů)	Průměrně **28.87** přístupů
Čtvrtky	**1119** přístupů (**15.17%** všech přístupů)	Průměrně **22.37** přístupů
Pátky	**1170** přístupů (**15.86%** všech přístupů)	Průměrně **22.93** přístupů
Soboty	**422** přístupů (**5.72%** všech přístupů)	Průměrně **8.27** přístupů
Neděle	**381** přístupů (**5.17%** všech přístupů)	Průměrně **7.62** přístupů

Používané prohlížeče :



Poměr Microsoft versus Zbytek světa je 84.1 : 15.9

Používané operační systémy :



Poměr Microsoft versus Zbytek světa je 95.5 : 4.5

Přeji hezký zbytek prázdnin a pěkně prožité dovolené.

Pavel Vondruška

B. Standardizační proces v oblasti elektronického podpisu v EU a ČR

Mgr. Dagmar Bosáková, Mgr. Pavel Vondruška (oba ÚOOÚ)
e-mail Dagmar.Bosakova@uoou.cz , Pavel.Vondruska@uoou.cz

Článek popisuje rozdílný normotvorný a standardizační proces v oblasti elektronického podpisu v EU a ČR.

I. Evropské společenství

Clara pacta – boni amici. (Jasné dohody – dobří přátelé.)

Evropský parlament a Rada přijaly v prosinci roku 1999 Směrnici o elektronických podpisech. Na základě tohoto dokumentu započaly rozsáhlé práce na přípravě národních zákonů o elektronickém podpisu v jednotlivých státech, resp. na sladění stávající legislativy s požadavky Směrnice.

Nejednalo se však pouze o započetí legislativních prací, ale i o rozsáhlé práce v oblasti přípravy příslušných norem a standardů. Již v lednu 1999 z podnětu Information Communications Technologies Standard Board (ICTSB) a za podpory Evropské komise zahájila činnost The European Electronic Signature Standardization Initiative (EESSI). Tato pracuje formou širokého diskusního fóra expertů ze sféry průmyslu, veřejné správy a dalších zainteresovaných subjektů. Jako výchozí principy této iniciativy byly přijaty zásady trvalé otevřenosti a transparentnosti činností a vyhlášena podpora vytvoření globálních a mezinárodně akceptovaných řešení v oblasti elektronického podpisu. Vedoucím skupiny EESSI se stal Claude Boulle (Bull, Francie).

Během necelých tří let svého působení prokázala *EESSI* schopnost účinně iniciovat a koordinovat přípravu a přijetí standardů nezbytných pro naplnění rámcových ustanovení Směrnice.

Pro operativnější práci bylo vytvořeno následujících dvanáct pracovních skupin (tzv. traiblazers TB1-TB12) : Public identity, Identification and authentiction, Protection profiles, security certification, Generalised card reader, Payment and m-payment, Contactless smart cards, Multi-application smart cards, User requirements, Public transport, e-Government, Health, Advanced Electronic Signature. Vlastní realizační práce spojené s vydáním potřebných standardů a norem jsou pak svěřovány evropským normalizačním organizacím, a to *CEN/ISSS (European Committee for Standardization / Information Society Standardization System)* a *ETSI (The European Telecommunications Standards Institute)***.**

Snad jedinou výjimkou je draft dokumentu Algorithm and Parametrs for Secure Electronic Signatures, který byl v květnu tohoto roku vydán přímo skupinou EESSI. Důvodem je možnost v případě potřeby reagovat rychleji než v klasickém procesu změny standardu či normy (např. z důvodu bezpečnosti odvolat používání některého algoritmu nebo možnost pozměnit doporučený parametr, či umožnit používání nového bezpečného algoritmu).

V krátkosti si představme obě výše jmenované evropské normalizační organizace.

ETSI (The European Telecommunications Standards Institute)

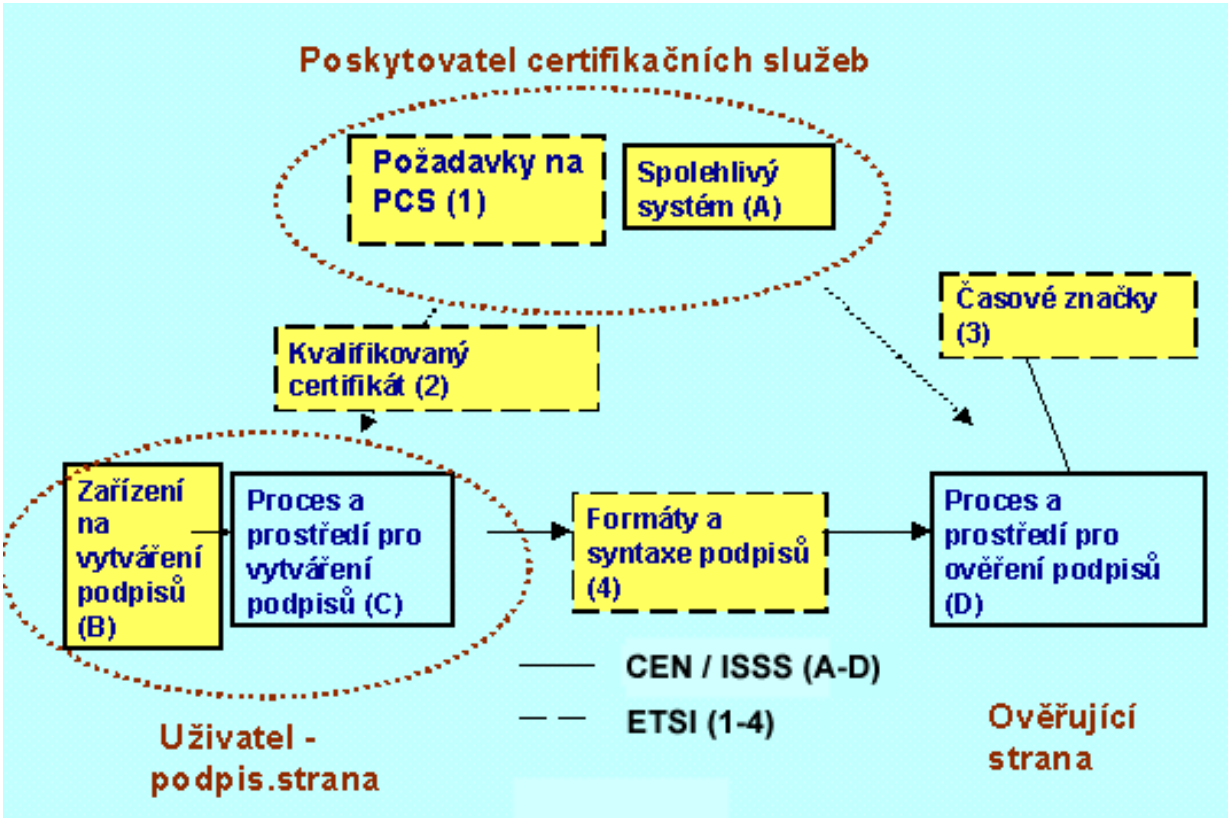
Jedná se o neziskovou organizaci, která působí od roku 1988 s cílem připravovat telekomunikační standardy pro dlouhodobé využití. Je oficiálně uznána jak Evropskou komisí, tak i sekretariátem EFTA (European Free Trade Association). Sdružuje více než 789

členů z 52 zemí reprezentovaných správními orgány, provozovateli sítí, servisními organizacemi, výrobci, výzkumnými pracovišti i uživateli. Standardizace prostředků elektronického podpisu, včetně standardů pro činnost podpůrných infrastruktur (PKI), je v kompetenci technické komise TC SEC (Security), v jejímž rámci byla ustanovena samostatná pracovní skupina pro oblast elektronického podpisu (Working Group on Electronic Signatures and Infrastructures - ESI WG). Jak již bylo řečeno, dokumenty (standardy) připravuje na základě podkladů a doporučení neformální odborné skupiny EESSI.

CEN/ISSS (European Committee for Standardization / Information Society Standardization System)

CEN/ISSS byl zřízen v roce 1997 Evropským výborem pro standardizaci (CEN) s cílem podpory informačních a komunikačních technologií v podmínkách rozvoje informační společnosti, kdy tradiční postupy standardizace a normalizace již nemusí zcela vyhovovat. CEN/ISSS je založen na přímé účasti výrobců, respektováním zájmů spotřebitele a principech otevřenosti a úplné transparentnosti. Vlastní realizační práce jsou organizovány v pracovních skupinách (Workshops), uspořádaných do pěti kmenových větví. Z toho ve větvi na podporu legislativního procesu je činná pracovní skupina pro elektronický podpis (E-SIGN Workshop). CEN/ISSS sídlí v Brusselu a v jeho čele je ředitel (John Ketchell) vybavený stálým sekretariátem.

Obrázek č.1 ukazuje, ve kterých oblastech se připravují příslušné normy a standardy, a jak je příprava rozdělena mezi CEN/ISSS a ETSI. Zatímco dokumenty CEN/ISSS jsou zaměřeny spíše na bezpečnostní aspekty praxe elektronického podpisu, otázky bezpečného prostředí a bezpečných podpisových a ověřovacích prostředků, dokumenty vydávané v rámci ETSI se týkají více formálních stránek problematiky. Tematicky jsou zaměřeny na problematiku kvalifikovaných certifikátů, problematiku časových značek a příslušné formáty z hlediska kompatibility a interoperability.



Legenda k obrázku č.1.
Dokumenty ETSI:
1) Policy Requirements for CSPs Issuing Qualified Certificates (ES[1], TS[2])
2) Qualified Certificates Profile (ES)
3) Time Stamping Profile (ES)
4) Electronic Signature Formats (EN[3])

Oblasti upravované dokumenty CEN/ ISSS:
A) Security requirements for trustworthy systems used by CSPs issuing qualified certificates
B) Security requirements for signature creation devices
C) User interface and operating environment for electronic signature creation
D) Signature Verification Process and Environment

V příloze č.1 je uveden přehled vydaných dokumentů ETSI (včetně typu a termínu vydání), v příloze č.2 jsou uvedeny některé důležité dokumenty CEN/ISSS. Příloha č.3 obsahuje současný legislativní stav v zemích ES.

II. Česká republika

Periculum in mora. (Nebezpečí z prodlení.)
Sua satius est mala quam alena tractare – Seneca. (Je lepší zabývat se vlastními nedostatky než cizími.)

A jaká je situace v ČR? V legislativním procesu naše republika za EU nezaostává. Zákon o elektronickém podpisu byl přijat 29. června 2000. Jeho účinnost byla stanovena k 1. 10. 2000. V současné době je v mezirezortním připomínkovém řízení návrh prováděcí vyhlášky k tomuto zákonu. Návrh vyhlášky upřesňuje podmínky stanovené v § 6 a § 17 zákona o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky. Návrh zpracovali pracovníci Úřadu pro ochranu osobních údajů (dále jen „Úřad“). Odborné aspekty byly konzultovány s členy odborné pracovní skupiny pro elektronický podpis. Členy této skupiny jmenoval předseda Úřadu RNDr. Karel Neuwirt. Složení této skupiny je dostupné na *http://www.uoou.cz/*. Obsah návrhu vyhlášky byl ve dvou kolech konzultován s odbornou veřejností. Konzultací se zúčastnili akademičtí pracovníci, lidé z praxe a další odborníci na informační bezpečnost a kryptologii. K vydání norem nebo standardů v oblasti elektronického podpisu nemá Úřad zákonné zmocnění.

Další legislativní podpora elektronického podpisu se očekává v podobě nařízení vlády (v době psaní tohoto článku ještě nebyla známa konečná podoba tohoto nařízení). Nařízení vlády bude řešit používání elektronického podpisu v oblasti veřejné moci. Toto nařízení rozvíjí paragraf § 11 zákona o elektronickém podpisu. K realizaci komunikace občan - stát zavádí nařízení tzv. elektronické podatelny. Následně se předpokládá vydání minimálně dvou standardů, které upraví bezpečnostní politiku takovýchto podatelen. První z nich stanoví technické parametry, druhý upraví vybavení elektronické podatelny. K vydání těchto standardů je podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy zmocněn Úřad pro veřejné informační systémy (ÚVIS – *http://www.uvis.cz*).

[1] ETSI Standard
[2] Technical Specification
[3] European Standard (Norm)

Dalším subjektem, který může svojí činností v ČR ovlivnit vydávání norem (standardů) v oblasti elektronického podpisu, je ČSNI (Český normalizační institut, *http://www.csni.cz/*). Plní funkci národní normalizační organizace v ČR. Rozhodující podíl na jeho normotvorné činnosti má zavádění evropských norem do soustavy ČSN. Tvorba norem čistě domácího původu tvoří v jeho činnosti cca 10 %. V oblasti, o níž hovoříme, připravuje převzetí důležitých ISO norem. Jmenujme zde alespoň ISO 17799 (Informační technologie - Soubor postupů pro řízení informační bezpečnosti) známá spíše jako British Standard - BS 7799 a dále ISO/IEC 15408 (Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií) známá spíše jako Common Criteria. Na obě připravované normy se odvolává i připravovaná vyhláška Úřadu k zákonu o elektronickém podpisu. Nejedná se ovšem o normy k elektronickému podpisu, ale normy z oblasti informační bezpečnosti. Standardy a normy odpovídající dokumentům ETSI nebo CEN/ISSS chybí.

Co zde v Čechách dále chybí, je iniciativa typu EESSI, která by se zabývala analýzou potřeb a následným vydáním, či doporučením k vydání příslušných metodik, norem a standardů, a to jak z hlediska možnosti převzetí již existujících dokumentů (z důvodu kompatibility, interoperability, ale i harmonizace legislativy), tak i z hlediska přípravy vlastních dokumentů.

Co dále chybí, je existence národního hodnotitelského pracoviště - technické laboratoře, která by prováděla odborná vyhodnocení, evaluaci a certifikaci kryptografických prostředků (včetně nástrojů elektronického podpisu, podpisových a ověřovacích prostředků). Ve Směrnici se předpokládá vznik takovéhoto pracoviště, které bude zapojeno do národního akreditačního schématu. Funkci hodnotitelského pracoviště může vykonávat i komerční subjekt. Výstavba hodnotitelského pracoviště je netriviální, dlouhodobou záležitostí, je třeba vysokých investic a potřeba získat řadu odborných pracovníků. Nelze se však tvářit, že takovéto pracoviště není nutné a jeho budování odkládat do doby našeho vstupu do EU.

III. Rozdíly a jak je prozatímně řešit ?

Bona fides exigit, ut, quod coventit, fiat.
(Dobrá vůle vyžaduje, aby bylo vykonáno, co bylo dohodnuto.)

Shrneme-li hlavní rozdíly v oblasti normotvorné a standardizační činnosti v EU a u nás, dojdeme k těmto závěrům :

- chybí silná, nezávislá, oficiálně uznaná odborná skupina, která inicializuje výběr a přípravu vhodných dokumentů (obdoba EESSI),
- chybí řada standardů technického a bezpečnostního charakteru (ekvivalent dokumentů ETSI a CEN/ISSS, RFC),
- chybí národní testovací laboratoř, resp. hodnotitelské pracoviště (zapojená do evropského akreditačního schématu).

Výše uvedené rozdíly jsou velice významné a mohou negativně ovlivnit používání elektronického podpisu. Podívejme se však ještě na jednu skutečnost. Jak a podle čeho poskytovatelé certifikačních služeb postupují, pokud musí řešit otázku technického rázu. V takovém případě vycházejí z dokumentů ETSI a CEN/ISS, případně ještě z dokumentů RFC. Je v jejich vlastním zájmu, aby jimi nabízená řešení byla kompatibilní a aby tak zajistili interoperabilitu s obdobnými řešeními v EU. Právě tato okolnost nás vede k představě dobrovolného přistoupení k připravované praxi v EU, tedy k tomu, že poskytovatelé

certifikačních služeb budou používat ve své činnosti platné dokumenty EU. K tomu je žádoucí vytvořit platformu odborníků, která bude konstatovat, zda příslušné dokumenty nejsou v rozporu s naším platným právním řádem, zejména zákonem o elektronickém podpisu a prováděcími předpisy, ale i nařízením vlády či standardy pro oblast veřejné správy . U některých dokumentů by tato platforma mohla iniciovat jejich převzetí (lze např. u dokumentů ETSI, které jsou označeny jako EN - European Standard (Norm)). Dokumenty, které nelze adoptovat do našeho právního řádu a které nejsou v rozporu s naší legislativou , pojmenovat a v podobě jakýchsi doporučení (obdoba best practices) doporučit k používání.. Jednotlivé subjekty by se pak ve své činnosti mohly na takto pojmenované dokumenty odvolávat a dobrovolně přistoupit na jejich používání. U naprosté většiny dokumentů se dá očekávat, že po vstupu do EU se stejně stanou pro nás závazné a je tedy vhodné se ve své činnosti jimi řídit již nyní. Velice cenné může být i konstatování, že příslušný dokument je v rozporu s naší stávající legislativou či praxí. Takováto konstatování mohou významně pomoci při přípravě harmonizačních prací, které nastanou při vstupu našeho státu do EU. Dokumenty ETSI a CEN/ISSS jsou totiž platné v rámci celé EU a příslušná legislativa musí být v souladu se Směrnicí.

Nepokládáme za vhodné, aby popsanou platformu vytvářel a řídil Úřad. Pomineme-li problematickou stránku zákonného oprávnění k vykonávání takové činnosti (zákon o elektronickém podpisu nepředpokládá, že by Úřad vykonával obdobnou činnost), zůstává otázka, zda je žádoucí, aby u jednoho subjektu byly kromě vydávání prováděcích předpisů, udělování akreditací a dozoru nad poskytovateli vydávajícími kvalifikované certifikáty koncentrovány další činnosti. Pokud však taková platforma vznikne, Úřad se nezříká spolupráce s ní.

Složitější je otázka vzniku hodnotitelského pracoviště. Může být zakomponováno do případné novely zákona o elektronickém podpisu, ovšem to je pouze legislativní stránka věci. Představa, že by vznik a fungování tohoto pracoviště byly hrazeny ze státního rozpočtu a prováděl je Úřad, patrně není ani realistická ani žádoucí. Komerční sféra má pro takovou činnost rozhodně lepší předpoklady. Lze tedy jen doufat, že pro firmy bude tato činnost natolik atraktivní, že o ni projeví zájem a že pro toto řešení bude možné vytvořit legislativní předpoklady.

Literatura:

[1] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, *http://www.ict.etsi.org/eessi/e-sign_directive.pdf*
[2] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) Sb. 227/2000, *http://www.uoou.cz*
[3] ETSI, European Telecommunication Standards Institute, *http://www.etsi.org/sec/el-sign.htm*
[4] CEN/ISSS, European Committee for Standardization / Information Society Standardization System, *http://www.ni.din.de*, *http://www.cenorm.be/isss/worksho/e-sign*
[5] EESSI, European Electronic Signature Standardization Initiative *http://www.ni.din.de* , *http://www.ict.etsi.org/eessi/EESSI-homepage.htm*
[6] Bosáková, D., Vondruška, P: Standardizační proces v oblasti elektronického podpisu v EU a ČR, DSM 4/2001, v tisku

Příloha č.1 – Přehled dokumentů ETSI

Type	TITLE	STATUS
Deliverable Type: **EN** Ref. **DEN/SEC-004001**	**Electronic signature formats**	**Drafting Stage** Current Status: **First complete draft (2000-09-07)** Next Status: **Start of WG approval process (2001-11-15)**
Doc. Nb. **ES 201 862** Ref. **DES/SEC-004003**	**Profile to qualified certificates based on RFC XXXX** Qualified certificate profile	**Drafting Stage** Current Status: **First complete draft (2000-09-07)** Next Status: **Start of WG approval process (2001-11-15)**
Doc. Nb. **ES 201 861** Ref. **DES/SEC-004004**	**Profile for protocol and format of time stamp based on RFC YYYY** Time stamping profile	**Drafting Stage** Current Status: **First complete draft (2000-09-07)** Next Status: **Start of WG approval process (2001-11-15)**
Deliverable Type: **TS** Ref. **DTS/SEC-004005**	**Security management and policy requirements for CSPs issuing time stamps**	**Drafting Stage** Current Status: **Start of work (2001-01-16)** Next Status: **Draft for public comment (2001-07-16)**
Deliverable Type: **TS** Ref. **DTS/SEC-004006**	**Policy requirements for CAs issuing other than Qualified Certificates**	**Drafting Stage** Current Status: **Start of work (2001-01-16)** Next Status: **Draft for public comment (2001-07-16)**
Doc. Nb. **ES 201 456** Ref. **DES/SEC-004007-2**	**Policies for CSP's** Policy requirements for certification authorities issuing qualified certificates	**Drafting Stage** Current Status: **First complete draft (2000-07-15)** Next Status: **Start of WG approval process (2001-11-15)**
Doc. Nb. **TS 101 903** Ref. **DTS/SEC-004008**	**Electronic Signature syntax and encoding formats in XML**	**Drafting Stage** Current Status: **Start of work (2001-01-01)** Next Status: **Stable draft (2001-07-16)**
Deliverable Type: **TS** Ref. **RTS/SEC-004009**	**Technical aspects of signature policies Informative annex to TS 101 733**	**Drafting Stage** Current Status: **Start of work (2001-01-16)** Next Status: **Draft for public commenting (2001-07-16)**
Deliverable Type: **TR** Ref. **DTR/SEC-004010**	**Infrastructure and interoperability requirements for provision of status information on Certification Service Providers**	**Drafting Stage** Current Status: **Start of work (2001-01-16)** Next Status: **Draft for public commenting (2001-07-16)**

Deliverable Type: **TR** Ref. **DTR/SEC-004011**	**Electronic Signature syntax and encoding formats in XML**	**Drafting Stage** Current Status: **Start of work (2001-01-31)** Next Status: **Stable draft (2001-07-16)**
Doc. Nb. **TS 101 862** Ref. **RTS/SEC-004012**	**Qualified certificate profile** Qualified certificate profile	**Drafting Stage** Current Status: **Draft receipt by ETSI Secretariat (2001-05-22)** Next Status: **Publication (2001-06-05)**
Doc. Nb. **TS 101 456** Ref. **RTS/SEC-004013**	**Policy requirements for certification authorities issuing qualified certificates**	**Drafting Stage** Current Status: **TB adoption of WI (2001-03-14)** Next Status: **Start of work (2001-07-01)**
Deliverable Type: **MI** Ref. **MI/SEC-004014**	**FAQ on Electronic signatures and Infrastructures standardization**	**Drafting Stage** Current Status: **Creation of WI by WG/TB (2001-03-14)** Next Status: **Start of work (2001-07-01)**
Deliverable Type: **TR** Ref. **DTR/SEC-004015**	**International Harmonization of Policy Requirements for CAs issuing Certificates**	**Drafting Stage** Current Status: **TB adoption of WI (2001-03-14)** Next Status: **Start of work (2001-07-01)**
Deliverable Type: **TR** Ref. **DTR/SEC-004016**	**Policy requirements for attribute authorities**	**Drafting Stage** Current Status: **TB adoption of WI (2001-03-14)** Next Status: **Start of work (2001-07-01)**
Deliverable Type: **TR** Ref. **DTR/SEC-004017**	**Signature policy for extended business model**	**Drafting Stage** Current Status: **TB adoption of WI (2001-03-14)** Next Status: **Start of work (2001-09-15)**
Deliverable Type: **MI** Ref. **MI/SEC-004018**	**Implementation of TS 101 733**	**Drafting Stage** Current Status: **Creation of WI by WG/TB (2001-05-16)** Next Status: **Start of work (2001-06-30)**

Příloha č. 2 – vybrané dokumenty CEN/ISSS WS/E

Area D1

N154 - Security Requirements for Trustworthy Systems
Managing Certificates for Electronic Signatures 13-06-2001

Area D2

N 1XX - Cryptographic Module for Certification Services – Protection Profile 21-06-2001

Area F

N137 - Secure Signature - Creation Device 01-03-2001

Area G1

N141 - Security Requirements for Signature Creation Applications 14-03-2001

Area G2

N 140 - Procedures for electronic signature verification 14-03-2001

Area V

N 128 - EESSI Conformity Assessment Guidance 23-01-2000

Příloha č. 3 – současný legislativní stav v zemích ES

Stát	Datum	Zákon
Belgie	**1997**	Adaptation of Belgian legislation to the Information Society
Dánsko	**10/2000**	Electronic Signature Act
Finsko	**1.1.2000**	Act on Electronic Service in the Administration
Francie	**29.2.2000**	Legislation on Electronic Signatures
GB	**19.6.2001**	Electronic Communications Act
Holandsko	**18.4.2001**	Draft Bill on Electronic Government Communications
Irsko	**7/2000**	Electronic Commerce Act 2000
Itálie	**15.4.1999**	Technical Rules for Digital Signatures
Lucembursko	**12.7.2000**	Digital Signature Law
Německo	**22.5.2001**	Digital Signature Law
Portugalsko	**2.8.1999**	Portuguese Digital Signature Law
Rakousko	**1.1.2000**	Electronic Signature Ordinance
Řecko	**?**	**?**
Španělsko	**9/1999**	Royal Decree on Digital Signatures
Švédsko	**1.1.2001**	Act on Qualified Electronic Signatures

C. XML signature

Jan Klimeš (student VŠE Praha, ORTEX, s.r.o. Hradec Králové)
e-mail j_klimes@ortex.cz

Poměrně novým fenoménem v informatice je popisný jazyk dat se vžitým jménem XML (eXtensible Markup Language). Tento článek se zabývá formátem XML signature – formátem digitálního podpisu ve struktuře jazyka XML.

1. XML

Formát jazyka XML je standardizován konsorciem W3C. V mnoha ohledech je tento formát podobný jazyku HTML. Základní rozdíl je v tom, že XML popisuje typ dat, nikoli vzhled dat v prohlížeči. XML dokument je tvořen párovými značkami – ‚tagy', které vyjadřují sémantiku dat. Jednotlivé tagy jsou do sebe vnořeny. Všechny elementy musí být na stejné úrovni ukončeny (omezení proti HTML). K dokumentu XML dále patří tzv. DTD a XML-schema. Ty slouží ke kontrole zadávaných údajů do XML dokumentu (lze přirovnat k doménové integritě v databázích). Jazyk XML je v současné době velmi progresivní, na jeho základě je budováno mnoho aplikací.

2. XML signature

XML signature je metoda, jakým způsobem spojit veřejný klíč, podpis a podepisovaná data. Nezabývá se přitom způsobem jakým je spojen veřejný klíč s podepisující osobou (lze řešit volitelnou položkou v *KeyInfo – X509Data*), ani smyslem podepisovaných dat. Na tomto místě je důležité podotknout, že podepsat lze jak dokument XML, tak jakýkoli jiný dokument. Z tohoto důvodu jsou rozlišovány tři typy XML podpisů: ***enveloped, enveloping a detached.***
Enveloped – podpis je součástí podepisovaného XML dokumentu. Před samotným ověřením podpisu je třeba provést transformaci XML dokumentu. Transformace vyjme podpis a posléze je dokument (či jeho část) ověřován. Zde se hovoří o tom, že XML podpis je „child".
Enveloping – podpis je „parent". Jedním z elementů XML podpisu je samotný podepisovaný XML dokument.
Detached – XML podpis je odděleným datovým prvkem nepřipojeným k podepisovanému XML dokumentu. Podepisovaný dokument je identifikovým odkazem (nemusí se jednat pouze o XML data) .

Pro jednotlivé algoritmy použité v XML-signature neexistují objektové identifikátory, ale jsou identifikovány pomocí **URI** (Unified Resource Identifier). Např. pro klíč typu DSA je to: http://www.w3.org/2000/09/xmlsig#DSAKeyValue.

2.1. Struktura

Základní struktura XML podpisu je tato:

```
<Signature>
  <SignedInfo>
    (CanonicalizationMethod)
    (SignatureMethod)
```

```
  (<Reference (URI=)? >
    (Transforms)?
    (DigestMethod)
    (DigestValue)
   </reference>)+
 </SignedInfo>
 (SignatureValue)
 (KeyInfo)?
 (Object)*
</Signature>
```

(? znamená 0 nebo 1; + znamená 1 a více; * zastupuje 0 a více)

2.2. SignedInfo

Element ***<SignedInfo>*** označuje, co a jakým způsobem je vlastně podepisováno. Nejdříve se věnujme elementu ***<Reference>***. Tento element obsahuje informace o tom, co je podepisováno.

- Nejjednodušší případ nastává, kdy reference je pouze jedna. Pak je vypočítána jedna HASH hodnota a ta podepsána
- Elementů <*Reference*> však může být více a pak je tedy vstupem pro podpisovou transformaci „složený dokument" (pro jeden každý dokument z referencí je počítán vzorek zprávy – pro ověření před podpisem).
- Reference může mít v sobě odkaz na vlastní objekt v ***<Object>*** části XML-sig schématu.
- Reference typu ***manifest*** odkazuje na uživatelský objekt v <*Object*> části a v tomto objektu typu manifest jsou reference na podepisované dokumenty. Tento typ je využitelný v případě, kdy nepotřebujeme, či nechceme počítat vzorek každého podepisovaného dokumentu, ale stačí nám kontrola celku. Využitelné je to v případě, kdy počítání vzorků je náročné. Druhou oblastí využití je situace, kdy mnoha klíči podepisuji mnoho dokumentů. Pak by bylo zbytečné udávat mnohokrát za sebou reference na ty samé dokumenty.

Než je dokument ze <*SignedInfo*> podepsán, je na něj uplatněna metoda tzv. **kanonikalizace**. Jedná o postup, kterým se uvede XML dokument pokaždé na stejný sled bytů před podpisem a před ověřením (podepsán a ověřován je tedy „kanonikalizovaný dokument"). Tímto algoritmem jsou řešeny problémy s jiným ukončením řádků (Unix a DOS formát), problémy s komentáři v dokumentu, které mohou, ale nemusí být též podepisovány. Kanonikalizace je řešena v samostatném standardu. Před vlastním podpisem mohou být provedeny ještě další transformace ***<Transforms>.*** Mezi ně patří: zašifrování/odšifrování, komprese/dekomprese, překódování (např. čeština), XSLT nebo Xpath. Poslední položkou v <*SignedInfo*> je <*DigestMethod*> a <*DigestValue*>. Metoda použitého hash algoritmu je opět identifikována pomocí URI (např. <DigestMethod Algorithm = http://www.w3.org/2000/09/xmldsig#sha1>). DigestValue je element v němž je pomocí BASE64 zakódován vzorek podepisovaného dokumentu.

2.3. SignatureValue

Element ***<SignatureValue>*** obsahuje hodnotu digitálního podpisu. Podpis je zakódován v BASE64. Ke správné interpretaci hodnoty podpisu vznikl datový typ *ds:CryptoBinary.* Jde o datový typ reprezentující velká čísla jako řetězec oktetů. Velké číslo je konvertováno do typu „big endian". Následně jsou zleva doplněny nuly, aby počet bitů byl dělitelný osmi. Pokud by řetězec bitů obsahoval na začátku nuly, pak bude zleva zkrácen, aby nebyl první oktet nulový. Takový oktet je potom zakódován BASE64.

2.4. Key Info

<KeyInfo> je volitelným elementem. Může obsahovat klíč nutný k ověření podpisu. V tomto elementu mohou být klíče, certifikáty, informace o PKI (například systém distribuce veřejných klíčů).
KeyInfo může obsahovat následující položky:
<*KeyName*> Řetězec identifikující klíč (může to být rozlišitelné jméno, či cokoli jiného)
<*KeyValue*> Zde lze nalézt jednotlivé veřejné klíče podepisující osoby. KeyValue může být buď DSAKeyValue nebo RSAKeyValue. Standard je sestaven tak, že lze doplnit vlastní klíčové informace - např. ECDSAKeyValue.
<*RetrievalMethod*> URI odkaz na místo, kde se nachází veřejný klíč.
<*X509Data*> Obsahuje identifikaci a certifikáty podle X.509. Může též obsahovat certifikační cestu až k ROOT CA. Obsahem může být DN podepisující osoby, DN vydavatele certifikátu a také celý certifikát v podelementu <*X509Certificate*>.
<*PGPData*> Element vytvořený pro možnost vložení klíče z programu Pretty Good Privacy (a kompatibilní).
<*SPKIData*> Použito pro vložení informace s SPKI veřejnými klíči, certifikáty.
<*MgmtData*> Informace použitelná pro distribuci klíčů (RSA šifrování klíčů, Diffie-Hellmanova výměna klíčů,…)

2.5. Postup při generování podpisu:

1. Příprava dat k podpisu
1.1. Aplikace metod <*Transforms*>
1.2. Vypočítání <*DigestValue*>
1.3. Vytvoření elementu <*Reference*> včetně identifikací algoritmů a hodnoty vzorku.

2. Tvorba podpisu
2.1. Vytvoření <*SignedInfo*> elementu (s metodami podpisu, kanonikalizací a referencemi)
2.2. Provedení kanonikalizace, vypočítání <*SignatureValue*> nad <*SignedInfo*>
2.3. Konstrukce <Signature> elementu nad elementy: <*SignedInfo*>, <*Objects*>, <*KeyInfo*> *a* <*SignatureValue*>.

3. Bezpečnostní hlediska

Z hlediska transformací je třeba podotknout, že podpis nad XML dokumentem podepisuje pouze to, co je výsledkem transformace (i když se vizuálně dokument nezměnil).

Z tohoto vyplývají následující „doporučení“ (dle mého názoru všeobecně platná, v tomto standardu explicitně vyjádřena):
Only what is signed is secure – podpisy nad transformovanými dokumenty nereflektují všechna původní data. Mimo algoritmus podpisu může stát například komentář.
Only what is „seen“ should be signed – pouze to, co je uživatel schopen vidět, zkontrolovat, atd. může být podepsáno.
„See“ what is signed - podobně jako v minulém požadavku, i zde je vyjádřeno, že pouze to, co je uživatel schopen zkontrolovat může být ověřeno.

V následující tabulce jsou algoritmy podporované podle standardu. Za povšimnutí stojí fakt, že zůstala pouze jediná hashovací funkce SHA-1. U každého algoritmu je jeho URI, kterým je algoritmus jednoznačně identifikován.

Typ algoritmu	Algoritmus	Požadavek	URI
HASH	SHA-1	REQUIRED	http://www.w3.org/2000/09/xmldsig#sha1
Kódování	BASE64	REQUIRED	http://www.w3.org/2000/09/xmldsig#base64
MAC	HMAC-SHA-1	REQUIRED	http://www.w3.org/2000/09/xmldsig#hmac-sha1
Signature	DSAwithSHA1 (DSS)	REQUIRED	http://www.w3.org/2000/09/xmldsig#dsa-sha1
	RSAwithSHA1	RECOMMENDED	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Kanonikalizace	Canonical XML with comments	RECOMMENDED	http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
	Canonical XML (omits comments)	REQUIRED	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Transformace	XSLT	OPTIONAL	http://www.w3.org/TR/1999/REC-xslt-19991116
	Xpath	RECOMMENDED	http://www.w3.org/TR/1999/REC-xpath-19991116
	Enveloped signature	REQUIRED	http://www.w3.org/2000/09/xmldsig#enveloped-signature

4. Závěr

V době odklonu informatického světa od binárních formátů vzniká tento formát elektronického podpisu. Jak bylo řečeno, nejedná se pouze o podepisování dokumentů XML, ale v tomto spojení (enveloped, enveloping XML signature) vidím největší budoucnost tohoto formátu. Zajímavé bude sledovat chování státu a jeho případná podpora tohoto standardu.

Podle vyjádření ing. Faltýnka z Ministerstva financí ČR budou daňová přiznání v první fázi podávána ve formátu XML souběžně s „papírovou“ verzí, v druhé fázi teprve uznávány elektronické podpisy. Není již pak důvod pouze rozšířit XML data o digitální podpis ve formátu XML.

Pojmy XML:

DTD Definice typu dokumentu - umožňuje automatickou kontrolu dokumentu.
XSL Jazyk pro transformace XML dokumentu (např. XML - HTML, XML do jiného XML schématu)
Xpath Metody pro získání pouze části XML dokumentu (filtrace)

Literatura:

[1] Úvod do XML od Jirky Koska (http://www.kosek.cz)
[2] W3C Candidate Recommendation 19-April-2001 - XML signature processing (http://www.w3.org/2000/09/xmldsig)
[3] Sborník konference ISSS (Internet ve státní správě a samosprávě) - 27.3.2001 Hradec Králové

Příklad elektronického podpisu ve formátu XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <Reference URI="http://nb.vse.cz/kmtp/TEST.htm">
   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
   <DigestValue>60NvZvtdTB+7UnlLp/H24p7h4bs=</DigestValue>
  </Reference>
 </SignedInfo>
 <SignatureValue>juS5RhJ884qoFR8flVXd/rbrSDVGn40CapgB...</SignatureValue>
 <KeyInfo>
  <KeyValue>
   <RSAKeyValue>
    <Modulus>uCiukpgOaOmrq1fPUTH3CAXxuFmPjsm...</Modulus>
    <Exponent>AQAB</Exponent>
   </RSAKeyValue>
  </KeyValue>
  <X509Data>
   <X509SubjectName>CN=Marta Klimesova,O=VSE
Praha,ST=Praha,C=CZ</X509SubjectName>
   <X509IssuerSerial>
    <X509IssuerName>CN=Test CA,O=ORTEX sro,ST=Hradec
Kralove,C=CZ</X509IssuerName>
    <X509SerialNumber>15658</X509SerialNumber>
   </X509IssuerSerial>
   <X509Certificate>MIICeDCCAeGgAwIBAgIEOd3...</X509Certificate>
  </X509Data>
 </KeyInfo>
</Signature>
```

D. O základním výzkumu v HP laboratořích v Bristolu, průmyslovém rozvoji a ekonomickém růstu

RNDr. Jaroslav Hrubý,CSc. (Fyzikální ústav AV ČR)
e-mail : hruby@gcucmp.cz

V malebné krajině v jižní části Anglie se nachází výzkumné laboratoře firmy Hewlett-Packard (HP), kde se vymýšlí nové technologie pro digitální budoucnost. Informační technologie nejsou jen katalyzátorem pro dynamický rozvoj lidské společnosti, ale podstatně urychlují i rozvoj základního výzkumu, a to i v takové oblasti jakou je kvantová fyzika.

HP laboratoře v Bristolu (HPLB) jsou největšími laboratořemi vně USA a zaměstnávají na 250 špičkových vědců a výzkumníků. Zaměřením HPLB je širokospektrální základní výzkum, a to nejenom v základních oblastech fyziky a matematiky, jehož výstupy jsou převáděny do aplikací pro informační systémy a technologie (IS/IT). HPLB spolupracují úzce s řadou obchodních partnerů firmy HP, ale především s universitami a akademickou obcí.

HP má vizi budoucnosti, kde technologie je dostupná všem ve světě učení, práce a poznání tak, aby každý měl prospěch z nových informací, a to v pozitivním smyslu.

Se vstupem do 21.století je více než kdykoliv předtím jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů u státní správy, zavést elektronické peníze a v neposlední řadě vytvořit infrastrukturu pro použití elektronického podpisu , jako jednoho se základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se tato zařadí mezi moderní, prosperující společnosti a udrží tempo rozvoje ve všech oblastech své činnosti, které je dáno globalizačními trendy.

Vizí HP je vytvořit takovouto společnost, ve které každý, kdo bude chtít, bude propojen se vším ostatním ve svém okolí a světě, kde triliony užitečných e-služeb jsou přístupné miliardám informačních uživatelů přes všudypřítomnou a vždy funkční informační infrastrukturu.

K dosažení této vize HP investuje obrovské finanční prostředky do výzkumu v následujících oblastech:

- výpočetní a internetové platformy
- e-služby a systémovou integraci s nimi související
- tiskové a zobrazující technologie pro informační systémy
- mobilní informační aplikace a osobní informační služby
- do nových směrů vědeckého výzkumu v oblastech molekulární elektroniky, kvantového počítání, kryptografie, nových médií pro ukládání informace a řady jiných souvisejících s IS/IT.

Ve svém článku se zaměřím na to, jak je propojen základní výzkum akademické obce s HPLB, jelikož se domnívám, že by to mohlo být inspirující pro spolupráci vysokých škol a akademie s komerčními firmami také v ČR.

V Bristolu využili tradiční model a umístili HP laboratoř, jejíž výstupy jsou aplikovány v průmyslu popřípadě přímo komerčně využívány, mezi administrativní divize HP a university, aby byl optimálně a pod dohledem zkušených manažerů, expertů na průmyslový rozvoj a ekonomický růst řešen problém inovátorského dilema. Co to je ?

Ukazuje se, že v posledních letech klasické inovační modely jsou nedostačující, jelikož se výrazně zkracuje inovační cyklus od základního výzkumu až k výrobku a objevuje se řada nových poznatků a vlivů inovační cyklus nejen urychlujících, ale i přerušujících (např. nový objev vedoucí k zcela jiným výrobkům, nebo změny na kapitálovém trhu znemožňující další financování výzkumného projektu pro jeho ekonomickou nevýhodnost apod.). Toto inovátorské dilema se neustále vyostřuje a nutí společnosti, aby hledaly řešení a predikovaly směry ve výzkumu, které ovlivní průmyslový rozvoj a ekonomický růst s předstihem. Obstojí ten, kdo přináší nové modely organizace výzkumu ve společnosti, které tuto dynamiku zohledňují. Pro ostatní zaostávající se stává výzkum ekonomicky neefektivním.

Pro optimální řešení inovátorského dilematu vznikl v HP Ústav základního výzkumu v matematických vědách, tzv.BRIMS (Hewlett-Packard`s Basic Research Institute in the Mathematical Sciences), který je vzorovým příkladem, jak průmysl společně s akademickou obcí jsou toto schopny řešit a predikovat směry výzkumu, ovlivňující průmyslový rozvoj i ekonomický růst, naplňovat vizi HP globální informační společnosti rovných mezi rovnými, vytvářet inkubátor nových talentů a myšlenek a ještě být pro společnost ekonomicky zisková.

Ekonomický zisk zdůrazňuji úmyslně, protože stejnou roli hraje zisk samotného poznání, intelektuálního růstu společnosti, nové objevy atd., který je rovněž významný. Nicméně na tento se mnozí u nás dívají jako na nějakou luxusní nadstavbu, kdežto ekonomickému zisku v tržní společnosti každý rozumí.

BRIMS lze charakterizovat jako partnerství HP a universit v Cambridgi a Bristolu, které umožňuje vytvářet možnost pro HP být inovátorem v takových oblastech jako jsou kvantové technologie a naopak pro university rozvíjet nový výzkum spojující oblasti matematiky, fyziky a počítačových věd. V BRIMS je rovněž vypracován postup pro výrazné talenty, jak kromě akademického růstu, spojit tento s kariérním růstem u firmy HP.

Příklad aplikace vědeckého výzkumu v oblasti kvantové informace jsme si vybrali jako jeden z mnoha řešených v BRIMS, na kterém se pokusíme čtenáři ukázat jak se výše zmíněné konkrétně realizuje.

Je dobře známo, že inovace tranzistorů a veškerý pokrok v této oblasti byl závislý na rozvoji v oblasti fyziky pevných látek. Během dalších deseti až patnácti let, pokud dynamika pokroku v této oblasti bude zachována, pokračující miniaturizace mikročipů dosáhne měřítek, kdy bude nutno započítávat efekty z kvantového světa.

Nové disciplíny týkající se kvantové teorie informace, se objevily na scéně v posledním desetiletí minulého tisíciletí a již podstatně změnili naše chápání fyziky, počítání a komunikací, ve kterých otevřely možnost absolutně bezpečného přenosu informací pomocí kvantové kryptografie.

Kvantová teorie informace a především kvantové počítání může však, kromě přínosu superrychlých počítačů, řešících složité matematické a fyzikální úlohy doposavad neřešitelné, také představovat principiální ohrožení klasických informačních systémů budovaných na informační infrastruktuře založené na asymetrické kryptografii.

Například digitální podpis využívá určitou matematickou vlastnost tzv. asymetrických šifrových systémů, založenou na složitosti matematických úloh faktorizace, diskrétního logaritmu a eliptických křivek. Soukromým klíčem se v digitálním podpisu nazývá posloupnost (řetězec) znaků, který umožňuje použít šifrování a pomocí hardwaru a softwaru realizovat podpis. Je zde použito asymetrické šifry, která obsahuje dva klíče, jeden klíč je určen pro zašifrování (nazývá se soukromý klíč) a jiný klíč slouží pro odšifrování (veřejný klíč). Přitom platí pravidlo, že ze znalosti veřejného klíče nelze odvodit klíč soukromý.

Zde existuje bezpečnostní riziko na samotné úrovni složitosti matematické úlohy faktorizace, která může být principiálně řešitelná pomocí kvantového počítače.

V kvantovém počítání existuje tzv. Shorův algoritmus, řešící úlohu faktorizace a Groverův vyhledávací algoritmus, který kvadraticky urychluje vyhledávání v databázích. Aplikace Groverova algoritmu by mohla kvadraticky urychlit přístup k potřebné informaci, a tak sehrát klíčovou roli pro urychlení vize HP propojeného světa e-služeb, jelikož rychlé vyhledání potřebných dat v gigabitech balastu je netriviální vědecký problém.

I když doposud technická realizace kvantového počítače operujícího s velkým počtem kvantových bitů neexistuje, je nutné i toto kvantové bezpečnostní riziko brát v úvahu již nyní a právě proto věnuje BRIMS kvantové teorii informace takovou pozornost, včetně napojení na koordinovaný výzkum kvantové informace v Evropské unii (EU).

Již dnes je odborníkům v EU zřejmé, že např. akreditovaná certifikační autorita archivující dle certifikační politiky kvalifikovaný certifikát, který je potřebný pro použití digitálního podpisu, a to po dobu delší, např. dvacet let, může být v tomto časovém horizontu kompromitována, jelikož tehdy již mohou kvantové počítače prakticky existovat.

Aby se předešlo možnému "Černému pátku" pro infrastrukturu založenou na šifrách s veřejným klíčem, který bude znamenat den praktické realizace kvantového počítače (kdy nejenže budou rozbity šifrové systémy stojící na složitosti faktorizace, ale i na složitosti diskrétního logaritmu a eliptických křivek, ale rovněž budou predikovatelné pseudonáhodné generátory, sehrávající podstatnou úlohu pro zabezpečení informací) je nezbytné hledání nových cest, jakými je např. kvantový kryptosystém s veřejným klíčem.

V HP laboratořích je dosaženo již řady konkrétních výsledků a kvantová kryptografie a kvantový generátor náhodných čísel mohou být komerčně realizovány v okamžiku ekonomické výhodnosti a nebo tehdy, kdy klasické systémy již nebudou bezpečné.

Vědci v BRIMS věnují nemalou pozornost zcela novému přenosu informace pomocí tzv. kvantové teleportace, využívající korelovaných kvantových fyzikálních stavů. Tento směr přináší nové možnosti kvantově kryptografických protokolů pro dosažení v limitě absolutní bezpečnosti, ale je zásadní i pro realizaci kvantových počítačů, například pro realizaci kvantových korekčních kódů na chyby vzniklé při aplikaci kvantového algoritmu.

Toto jsou právě příklady predikce nových směrů ve výzkumu, které pozitivně ovlivní průmyslový rozvoj a ekonomický růst společností , které tyto směry zvládnou s předstihem.

Je možné namítnout, že technologický přechod k využití kvantové teorie informace pro široké praktické využití je vědecky daleko náročnější a ekonomicky nákladnější, než tomu bylo u přechodu využití poznatků fyziky pevných látek pro praktické použití polovodičů, tranzistorů a mikročipů. To je bezpochyby pravda, ale ten kdo tuto vlnu rozvoje nepodchytne může zaostat, jak známe z historie, a jako pouhý spotřebitel produktů nové technologie v tržním světě v konečné fázi zaplatit mnohonásobně cenu výzkumu i vývoje společnostem, které jej realizovaly.

BRIMS nejen tuto vlnu podchycuje a nese zdravou míru rizika v predikci úspěšnosti a realizovatelnosti tohoto směru, ale je svými vedlejšími produkty (např. průběžnými získanými poznatky, aplikovanými pro bezpečnost informací, prodejem a pronájmem "mozků" svých vědců apod.) ekonomicky zisková.

Závěrem si dovolím požádat čtenáře a i naši akademickou obcí, aby se zamysleli nad tímto příkladem, popřípadě se jím inspirovali a pokoušeli se podobná partnerství mezi komerčními firmami a akademickou obcí budovat v ČR v daleko větším měřítku, než se děje doposud.

E. Letem šifrovým světem - přehled vybraných akcí

1. Skljarov (ElcomSoft) zatčen za šíření demoverze programu ke čtení zabezpečených elektronických knih !
Mgr. Pavel Vondruška (ÚOOÚ)

Dne 16.7. byl na tradičním srazu hackerů v Las Vegas (Def Con, 500 účastníků) zadržen pracovníky FBI, 26letý ruský programátor Dmitrij Skljarov. Tento mladý Rus byl zatčen za prodej softwaru zaměřeného na rozbití kódu, který chrání elektronické knihy (konkrétně eBook Reader, produkt firmy Adobe) proti otevření neoprávněným uživatelem. Byl zadržen na základě nového amerického (veřejností kritizovaného) zákona proti počítačovým pirátům (U.S. anti-piracy laws - the Digital Millennium Copyright Act.). Hrozí mu vězení ve výši 5 let a pokuta půl miliónů dolarů. Skljarov pracuje pro Moskevskou firmu ElcomSoft Co.

Firma byla založena roku 1990 a specializuje se na výrobu softwaru, včetně produktů určených pro obnovu ztracených hesel pro různé aplikace. Prezident společnosti Alexandr Katalov, který se také setkání v Las Vegas zúčastnil, řekl: "Dmitrij byl jedním ze tří programátorů, kteří se na psaní programu podíleli. Copyright na tento software drží naše firma ElcomSoft. Jsem velmi překvapen, že byl Dmitrij zavřen." Katalov dále řekl, že firma prodala 500 CD s trial verzemi svých programů, včetně programu, který umožňuje prolomit šifrovou ochranu produktu eBook Reader od Adobe. Současně upozornil, že se odemkne pouze 25% ze zašifrované elektronické knihy. Dále program požaduje správné zadání hesla a teprve potom lze vytvořit kopii knihy, která je již potom dále volně kopírovatelná. Použít program tedy může pouze legální uživatel elektronické knihy. Katalov upozornil, že plánované využití programu bylo určeno pouze k vytvoření kopie knihy např. pro domácí počítač nebo na notebook. Tedy pouze pro potřeby oprávněného uživatele, který za "odemknutí" zašifrované knihy řádně zaplatil.

Skljarovova prezentace, předvádějící, jak je lehké zlomit ochranu firmy Adobe, je dostupná na http://www.treachery.net/~jdyson/ebooks/ . Vladimir Katalov v e-mailu zaslaném na adresu Crypto-Grammu popisuje (ještě před zatčením Skljarova !), jak „rozbili“ původní DRM od Adobe (též nazývané „digital copy protection scheme“). Zveřejněný útok umožňuje odstranit všechny ochrany, které zajišťoval tento systém při vytváření PDF souborů (určených k distribuci v podobě elektronické knihy). Firma Adobe reagovala „odstraněním“ zveřejněných děr a vytvořila novou verzi na ochranu svých dokumentů. Tuto novou verzi firma ElcomSoft opět „rozbila“, tentokráte za dvacet minut …. Demo tohoto nového útoku bylo součástí CD, které Skljarov za 99 dolarů prodával na konferenci v Las Vegas a za jehož prodej byl zatčen.

Popis „bitvy“ mezi firmou ElcomSoft a Adobe (včetně demonstračního programu, který byl stále ještě v době psaní tohoto příspěvku dostupný) je na
http://www.elcomsoft.com/aebpr.html

Další informace k celému případu lze získat např. na
http://www.wired.com/news/politics/0,1283,45298,00.html

2. FIPS PUB 140-2, bezpečnostní požadavky na kryptografické moduly

Ing. Jaroslav Pinkava, CSc., (Norman Data Defense System CZ & AEC spol. s r.o.¨)

Problematika hodnocení bezpečnostních vlastností kryptografických produktů patří k těm poměrně náročným činnostem. Tyto činnosti jsou však naprosto nezbytné. Je to zejména proto, že zákazník, uživatel bezpečnostních technologií (zde tedy kryptografického prostředku), chce a to zcela oprávněně, být ubezpečen, že daný prostředek plně poskytuje požadovaný stupeň jistot [6].

Na začátku července 2001 bylo NIST (National Institute of Standards and Technology – USA) oznámeno schválení nové verze známé normy FIPS-140 (datum vydání uvedené v samotném dokumentu je 25. květen 2001). Tato podoba normy nahrazuje předchozí verzi FIPS PUB 140-1 z ledna 1994. Základní informace o normě lze nalézt na adrese [1] , samotnou normu pak na adrese [2] . Draft FIPS-140-2 byl zveřejněn již v roce 1995 a byl tak podroben široké diskusi.

Nesporně zajímavým dokumentem je [3] , které přináší podrobné srovnání obou verzí FIPS 140, tj. verze FIPS 140-1 a FIPS 140-2.

Bezpečnostní požadavky v normě obsažené jsou rozděleny do 11 oblastí a hodnoceny dle čtyř úrovní bezpečnosti (s postupně narůstajícími nároky). To platí pro obě verze normy. Jak však lze vidět z následující tabulky, pozměnil se obsah těchto oblasti:

FIPS 140-1	FIPS 140-2
4.1 Cryptographic Modules	4.1 Cryptographic Module Specification*
4.2 Cryptographic Module Interfaces	4.2 Cryptographic Module Ports and Interfaces
4.3 Roles and Services	4.3 Roles, Services, and Authentication*
4.4 Finite State Machine Model	4.4 Finite State Model
4.5 Physical Security	4.5 Physical Security*
4.6 Software Security	4.6 Operational Environment*
4.7 Operating System Security	4.7 Cryptographic Key Management
4.8 Cryptographic Key Management	4.8 EMI/EMC
4.9 Cryptographic Algorithms	4.9 Self-Tests*
4.10 EMI/EMC	4.10 Design Assurance*
4.11 Self-Tests	4.11 Mitigation of Other Attacks*

Přitom odstavce označené hvězdičkou byly zcela přepracovány, nebo doznaly význačných změn.

Změny vychází v převážné většině z nezbytnosti reagovat na existenci nových technologií či nových bezpečnostních požadavků (např. autentizace v paragrafu 4.3 atd). V odstavci 4.6 dochází k významné změně v odkazu na hodnocení bezpečnosti informačních systémů. Zatímco dříve se norma odkazovala na TCSEC, odkazuje se FIPS 140-2 již na Common Criteria. Odstavec 4.11 je vlastně nový (došlo k přesunu jiných odstavců) a jeho význam spočívá v tom, že metodika zde umožňuje reagovat na řadu kryptografických útoků, které se objevily teprve v poslední době (jako jsou analýza spotřeby proudu, časová analýza, analýza vynucených chyb atd.).

Pokud čtenáře zajímají již evaluované produkty, pak jejich seznam lze nalézt na adrese [4] . Vzhledem k teprve velice nedávnému zavedení normy FIPS 140-2 lze zde ovšem nalézt zatím pouze produkty evaluované dle FIPS 140-1 (stav k 20. červenci 2001). V současné době pracuje v USA a v Kanadě pět komerčních evaluačních laboratoří [7] , které do dnešního dne vyhodnotili pozitivně zhruba 150 kryptografických produktů. Nyní laboratoře testují (do května 2002) souběžně dle obou verzí normy (140-1 a 140-2), od května 2002 to bude již výlučně dle normy FIPS 140-2.

NIST a CES (obdobná kanadská instituce) v současné době připravují příručku (FIPS 140-2 Implementation Guidance) pro výrobce kryptografických modulů a testovací laboratoře. Rovněž tak je připravována nová verze dokumentu FIPS 140-2 Derived Test Requirements.

Odkazy:

[1] http://csrc.nist.gov/cryptval/140-2.htm
[2] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[3] http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf
[4] http://csrc.nist.gov/cryptval/140-1/1401val.htm
[5] Honigová, Alena: Bezpečnostní požadavky pro kryptografické moduly, DSM 6/2000
[6] Pinkava, J.: Certifikace kryptografických prostředků a prostředků pro elektronický podpis, DSM 6/2000
[7] http://csrc.nist.gov/cryptval/

3. Faktorizace velkých čísel - nová podoba výzvy RSA

Ing. Jaroslav Pinkava, CSc., (Norman Data Defense System CZ & AEC spol. s r.o.)

V polovině června 2001 oznámily RSA Laboratories, výzkumné středisko společnosti RSA Security novou podobu své již deset let běžící výzvy pro faktorizaci velkých čísel. Oproti dřívější podobě došlo k následujícím výrazným změnám:

1) byla zjednodušena celá struktura výzvy, v současné podobě existuje jeden relativně krátký seznam osmi čísel, která jsou předložena k faktorizaci; přitom byla do seznamu zařazena nyní i čísla delší - nejkratší číslo má 576 bitů, nejdelší má 2048 bitů;

2) byly zvýšeny odměny za provedené faktorizace – pohybují se od deseti do dvou set tisíc dolarů

Z tiskové zprávy:

"RSA Factoring Challenge se historicky osvědčila jako vynikající podnik pro výzkumníky z celého světa, který nabízí cenné a pronikavé příspěvky do aktuálního souboru znalostí v odvětví IT bezpečnosti," řekl Burt Kaliski, vedoucí vědecký pracovník RSA Laboratories. "Nabízené peněžní ceny jsou míněny jako ocenění namáhavé práce, věnované koordinaci prostředků a úsilí potřebného k překonání některých velmi obtížných technických překážek, s nimiž se setkáváme na poli faktorizace velkých číselných hodnot."

Pro zájemce uvádíme alespoň nejkratší a nejdelší číslo obsažená v této výzvě:

RSA-576 Cena: $10000 Počet číslic: 174 Kontrolní součet číslic: 785
188198812920607963838697239461650439807163563379417382700763356422988859715
234665485319060606504743045317388011303396716199692321205734031879550656996
221305168759307650257059

RSA-2048 Cena: $200000 Počet číslic: 617 Kontrolní součet číslic: 2738
251959084756578934940271832400483985714292821262040320277771378360436620207
075955562640185258807844069182906412495150821892985591491761845028084891200
728449926873928072877767359714183472702618963750149718246911650776133798590
957000973304597488084284017974291006424586918171951187461215151726546322822
168699875491824224336372590851418654620435767984233871847744479207399342365
848238242811981638150106748104516603773060562016196762561338441436038339044
149526344321901146575444541784240209246165157233507787077498171257724679629
263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357

Zatím největší faktorizované číslo obecného tvaru (pro speciální čísla v podobě např. 2^n +1 byly dosaženy ještě lepší výsledky) je RSA-155 (512 bitů, 155 dekadických čísel). Tato faktorizace proběhla v srpnu 1999 a čtenáři byly o ni informování v jednom z prvních čísel Crypto-Worldu.

Přehled dosažených výsledků při faktorizaci obecných čísel (výzvy RSA)

Číslo	**Datum**	**MIPS-roků**	**Dnů P II/450**	**Metoda**
RSA-100	Duben 1991	7	5,67	Quadratic-sieve
RSA-110	Duben 1992	75	60,8	Quadratic-sieve
RSA-120	Červen 1993	830	673	Quadratic-sieve
RSA-129	Duben 1994	5000	4055 (11 let)	Quadratic-sieve
RSA-130	Duben 1996	500	405,5	Generalized number field sieve
RSA-140	Únor 1999	2000	1622,2 (4,5)	Generalized number field sieve
RSA-155	Srpen 1999	8000	6488,8 (17 let)	Generalized number field sieve

Odkazy:
Další informace vzhledem k výzvě lze nalézt na webovské stránce:
http://www.rsasecurity.com/rsalabs/challenges/factoring/index.html.
V současné době nejlepší známou faktorizační metodou je General Number Field Sieve (viz např. známý RSA FAQ - http://www.rsasecurity.com/rsalabs/faq/2-3-4.html).

K faktorizaci dále viz. též série článků P.Vondrušky ve starších číslech Crypto – Worldu:
Fermatova čísla , http://mujweb.cz/veda/gcucmp/casop2/crypto4_00.html
Mersennova prvočísla , http://mujweb.cz/veda/gcucmp/casop2/crypto5_00.html
Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla I. ,
http://mujweb.cz/veda/gcucmp/casop2/crypto6_00.html
Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla II. ,
http://mujweb.cz/veda/gcucmp/casop2/crypto78.html
Je RSA bezpečné?, http://mujweb.cz/veda/gcucmp/casop4/Crypto_1.html
Viz též - http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa155.html.

4. NOVÁ DIREKTIVA EU ...

Na broskve se šuplérou

17.7.2001

http://www.novinky.cz/Index/Boulevard/8280.html?from=seznam_hp

Podle direktivy EU musejí mít broskve prodávané v období od 1. července do 31. října v průměru alespoň 56 mm. Londýnská rozhlasová stanice Magic zvěstovala tuto zprávu jako další ukázku šílenosti bruselských úředníků. Lord Morris se členům Sněmovny lordů svěřil, že obvykle s sebou nenosí metr, když kupuje ovoce. Další člen parlamentu sir Teddy Taylor uvedl, že v roce 1998 bylo kvůli přebytkům v EU zničeno více než 90 000 tun broskví. "Toto nesmyslné nařízení způsobí, že broskve budou znovu ničeny a daňoví poplatníci to opět zaplatí," dodal.

... a její možný dopad

Exkluzivně z Brna pro Crypto-World Jaroslav Pinkava

V dobře informovaných novinářských kruzích v Bruselu probleskují zprávy o nových převratných kryptografických metodách. Tyto metody jsou vytvářeny na bázi nového principu, který je zatím přísně utajován. Co se zatím podařilo novinářům zjistit je nečekaná souvislost s dosud zcela odlišným hospodářským odvětvím - produkcí broskví. Zjistit se podařilo novinářům ještě jednu zajímavou okolnost. Bezpečnost (nebo také odolnost) nových kryptografických postupů je přímo úměrná velikosti použité broskve. Zkrátka čím větší broskev, tím vyšší stupeň kryptografické odolnosti. Standardem v první fázi budou 56 mm broskve (nepotvrzené dohady poukazují na souvislost s délkou klíče u americké normy DES - 56 bitů). Podle některých odborníků to však stačit nebude a bude nezbytné přejít na minimální velikost broskví 128 mm a v záloze by měly již být připraveny i 256 mm broskve. Teprve takto veliké broskve jsou prý podle odborníků schopny poskytnout požadovanou bezpečnost.

Ovšem zároveň se objevila jiná zpráva (upozorňujeme čtenáře, že její pravdivost teprve prověřujeme) o jiném výzkumu, který v Bruselu nedávno proběhl. Tento výzkum se zabýval intelektuálními schopnostmi bruselských úředníků a jedním z jeho velice zajímavých výsledků je prý nalezená statistická korelace mezi IQ úředníků a velikostí jimi pojídaných broskví. Čím větší broskev, tím inteligentnější úředník. Zlé jazyky ovšem tvrdí, že korelace je výsledkem jiných faktorů, protože větší broskve jsou dražší, mohou si je koupit pouze úředníci s vyššími platy a u těch je vyšší IQ jaksi předpokládán. Toto tvrzení však vyvrací včera zveřejněná fotografie jednoho vysokého komisaře EU, který byl vyfotografován, jak se vrací z tržiště obtěžkán dvěma velikými taškami plnými broskví. Z fotografie je zcela zjevně vidět, že velikost žádné broskve nepřesáhla 30 mm.

Ptáme se tedy: kde je pravda? Dozví se naši čtenáři, co vše se skrývá za zákulisními boji o velikost broskví? A co na to naši poslanci, dokážeme i my v České republice přijmout včas potřebnou legislativu?

5. Upozorňuji na blížící se mezinárodní databázovou konferenci DATAKON 2001. Termín a místo konání : 20. - 23.10.2001, Hotel SANTON, Brno. Podrobné informace najdete na -> http://www.datakon.cz

6. Firmy, které pronajímají auta, používají GPS ke sledování svých zákazníků. Tento postup je označen za nedovolený.
   http://www.zdnet.com/zdnn/stories/news/0,4586,2778752,00.html
   http://www.zdnet.com/zdnn/stories/news/0,4586,5093616,00.html
   http://www.wired.com/news/privacy/0,1848,45163,00.html

7. O tom, jak hackeři (a to třeba ještě i děti) umí zneužít to, že správci systémů nenainstalovali včas příslušný bezpečnostní patch pro Microsoft IIS.
   http://news.cnet.com/news/0-1003-200-6353491.html?tag=mn_hd

8. Seznam hlavních obecných bezpečnostních chyb (Top 10 security mistakes).
   http://www.idg.net/ic_646834_1794_9-10000.html

9. Porovnání „biologických" virů s počítačovými viry.
   http://securityportal.com/articles/greatanalogy1.html

10. 27.7.2001 předal americký prezident ocenění posledním pěti žijícím indiánům Navajům, kteří za druhé světové války předávali pomocí smluvené řeči (kódové knihy) ve svém rodném jazyce šifrové zprávy. Současně se v amerických kinech začal promítat film o jejich hrdinských činech. O osudech, činech a o systému předávání zpráv jsme psali v našem Crypto-Worldu již před rokem. Viz. články:
    Vondruška,P. : Code Talkers (I.díl), Crypto-World 4/2000
    Vondruška,P. : Code Talkers (II.díl), Crypto-World 5/2000
    Vondruška,P. : Code Talkers (III.díl), Crypto-World 6/2000
    Přílohou ke Crypto-Worldu 6/2001 byla odtajněná kódová kniha, kterou Navajové používali. Jednalo se o revizi z 15.6.1945.

11. O čem jsme psali před rokem ?
    Crypto -World 7-8/2000
    http://www.mujweb.cz/veda/gcucmp/casop2/Crypto78.html
    A. Ohlédnutí za I.ročníkem sešitu Crypto-World (P.Vondruška) 2-4
    B. Kryptosystém s veřejným klíčem XTR (J.Pinkava) 4-6
    C. Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla (P.Vondruška) 7-9
    D. Počátky kryptografie veřejných klíčů (J.Janečko) 10-14
    E. Přehled některých českých zdrojů - téma : kryptologie 15-16
    F. Letem šifrovým světem 17-18
    + příloha : 10000.txt (Seznam prvních 10 000 prvočísel)

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "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.

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

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.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@uoou.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@uoou.cz (**vondruskap@uoou.cz**)

vondruska.p@seznam.cz

pavel.vondruska@post.cz