Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 3, číslo 12/2001 **18. prosinec 2001**

12/2001

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
(>330 e-mail výtisků)

Obsah : **Str.**

Příloha: uloha7.wav

A. Soutěž 2001 , IV.část

Pavel Vondruška, ÚOOÚ

Dospěli jsme k poslední části naší soutěže v luštění různých jednoduchých problémů souvisejících se základními šifrovými systémy. I letošní soutěž (podobně jako loňská) proběhla ve čtyřech kolech. V každém ze sešitů 9/2001 až 12/2001 byla uveřejněna jedna nebo dvě soutěžní úlohy a současně uveden doprovodný text k této úloze. Řešitelé, kteří zašlou správné řešení do 30.12.2001, budou slosováni a vítěz získá cenu kola. Cenou kola je CD se staršími čísly Crypto-Worldu a placený certifikát od některého z předních poskytovatelů těchto služeb.

Celkovým vítězem se stane ten řešitel, který vyluští správně všechny vyhlášené úlohy a jejich řešení zašle do 30.12.2001. Stále tak máte možnost se zapojit do soutěže a stát se celkovými vítězi. Stačí jen zaslat v daném časovém limitu všechna příslušná řešení. První číslo e-zinu v roce 2002 bude věnováno vyhodnocení soutěže. Mimo jména vítěze budou uvedena řešení úloh všech kol. Hlavní cenu soutěže věnoval jeden z loňských úspěšných řešitelů. Cena je velice lákavá - šest lahví kvalitního značkového bulharského vína ve speciálním balení připraveného pro tuto soutěž (foto viz. Crypto-World 11/2001).

Připomeňme, jaké úlohy byly čtenářům předloženy v předchozích kolech:

Září	- jednoduchá záměna , kódová kniha
Říjen	- absolutně bezpečný systém
Listopad	- jednoduchý šifrový systém, RSA

Řešitel	I.kolo 1.úloha	I.kolo 2.úloha	II.kolo 3.úloha	III.kolo 4.úloha	III.kolo 5.úloha	IV.kolo 6.úloha	IV.kolo 7.úloha
František P.	19.09/10	19.09/10	16.10/10	15.11/10	15.11/10		
Jan J.	19.09/10	19.09/10	18.10/10	15.11/10	15.11/10		
Mirek Š.	30.10/10	30.10/10	30.10/10	19.11/10	19.11/10		
Jan Kl.	20.11/10	20.11/10	30.10/10	20.11/10	16.11/10		
Jozef K.	02.10/10	02.10/10		16.11/10	16.11/10		
Martin K.		19.11/10	20.11/ 10	19.11/10	19.11/10		
Vítězslav S.		6.11 /10	6.11 /10	19.11/10	19.11/10		
Tomáš V.	21.10/10	26.09/10		16.11/10	16.11/10		
Karel Š.	10.10/10	10.10/10	31.10/10				
Jan K.		30.09/10	21.10/10		17.11/10		
Ivan S.	14.11/10	14.11/10	14.11/10				
Richard K.	04.10/10	04.10/10					

Všechny řešitele prosím o kontrolu, zda jsou v tabulce zanesena všechna jimi odeslaná řešení. Pokyny pro řešitele, kteří vyluští všechny úlohy:

- dnešní úlohy zašlete do 30.12.2001 a označte je dle pokynů uvedených za zadáním úlohy
- dále zašlete e-mail (předmět : losovani o celkoveho viteze)
- v tomto e-mailu uveďte libovolné číslo od 0 do 100 !
- uveďte své celé jméno a příjmení (v případě, že budete vylosován jako celkový vítěz, bude zveřejněno) a město, ve kterém bydlíte (nebude zveřejněno)
- ke komunikaci použijte adresu pavel.vondruska@post.cz a kopie zašlete na adresy vondruska.p@seznam.cz a pavel.vondruska@uoou.cz

Způsob určení celkového vítěze:

Po kontrole oprávněnosti vašeho zařazení do losování o celkového vítěze soutěže vám bude přiděleno pořadové číslo. Vámi zaslané celé číslo od 1 do 100 se přičte k číslům, která zašlou ostatní řešitelé. V případě, že žádné číslo nezašlete nebo nebude z intervalu 1-100, přičte se k ostatním číslům vaše pořadové číslo. Tato čísla zveřejníme. Výběr celkového vítěze pak proběhne takto - označme S celkový součet všech čísel zaslaných úspěšnými řešiteli (předpokládejme, že řešitelů bude N). Vypočteme $V \equiv S \bmod N$. Hodnota V+1 pak určí celkového vítěze (nabývá hodnot od 1 do N ☺).

Jak získat podpis k textu od jiné osoby

Nejprve doporučuji přečíst článek "Asymetrická kryptografie - RSA", který vyšel v minulém čísle našeho e-zinu. Tato část na něj volně navazuje. Zatímco v minulém čísle jsme se věnovali popisu algoritmu RSA, definici šifrování a dešifrování a zakončili jsme úkolem najít klíč na dešifrování tajné zprávy, dnes se budeme věnovat útoku na podpis, který je založen na použití RSA.

Předvedeme si, jak lze za jistých okolností získat podpis nějaké osoby pod (námi připravený) text, aniž by ve skutečnosti daná osoba text podepsala.

Pro srozumitelnost výkladu zvolme následující jednoduché podpisové schéma. (Útok však lze realizovat v určitých obměnách i na skutečně používaných podpisových schématech SHA1/RSA, MD5/RSA apod.).

Podpisové schéma RSA

(V podstatě se jedná o klasické podpisové schéma, kde je však vynechána hashovací funkce a text není formátován podle PKCS #1.0).

Vyjdeme z klasického RSA. Zvolíme prvočísla p a q a vypočteme

$N = p*q$

$\Phi(N) = (p-1)*(q-1)$

Dále zvolíme náhodné číslo e, kde

$1 < e < \Phi(N)$, takové, že e a $\Phi(N)$ jsou nesoudělná.

Vypočteme číslo d takové, že

$1 < d < \Phi(N)$ a

$e*d \equiv 1 \bmod \Phi(N)$.

Dvojici (N,d) nazveme soukromý - tajný - podpisový klíč a (N,e) veřejný klíč - data na ověření podpisu.

Podpis zprávy M

Zprávu M překódujeme nejprve do číselného tvaru. K tomu použijeme některou vhodnou převodovou tabulku. Např. upravenou tabulku z minulého čísla:

	0	1	2	3	4	5	6	7	8	9
6	**0**	**Mezera**	**2**	**3**	**4**	**A**	**B**	**C**	**D**	**E**
7	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
8	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
9	**Z**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Zprávu M pak zformátujeme do posloupnosti čísel pevné délky (délka bude rovna délce modulu N). K tomu použijeme nepatrně upravené formátování Crypto#1.0, které jsme zavedli v minulém čísle našeho e-zinu. Nazvěme je formátování Crypto#1.12:

Formátování Crypto #1.12 :
1) Má-li modul délku k, budeme zprávu v dekadickém tvaru dělit na skupiny délky k-1.
2) Všechny skupiny musí mít délku k-1, nemá-li poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
3) Skupiny nyní doplníme zleva jednou nulou. Délka každé skupiny je tedy rovna k.
4) Výsledek po podpisové transformaci má délku rovnou maximálně k, nemá-li ji doplníme výsledek zleva nulami.

Získaný výsledek po formátování M označme $M= m_1\ m_2\ m_3\ \ldots..$

Podpisem zprávy M pak nazveme řetězec
$M = C_1\ C_2\ C_3\ .....$, kde
$C_1 \equiv m_1^d \bmod N$, $C_2 \equiv m_2^d \bmod N$, $C_3 \equiv m_3^d \bmod N$ ..... $C_i \equiv m_i^d \bmod N$

Ověření podpisu zprávy M se pak provede tak, že vypočteme pomocí dat na ověření podpisu následující výrazy
$V_1 \equiv C_1^d \bmod N$, $V_2 \equiv C_2^d \bmod N$, $V_3 \equiv C_3^d \bmod N$ .... $V_i \equiv C_i^d \bmod N$

Pokud $V_i = m_i$ pro všechna i, řekneme, že ověření podpisu bylo úspěšně provedeno.

Pokud podepisující osoba dokáže udržet svá data na podepisování v tajnosti (a čísla p a q byla dostatečně velká), pak je výpočetně složité ze znalosti podpisu zprávy a dat na ověření podpisu vypočítat soukromý – podepisovací klíč.

Nyní si ukážeme, jak lze získat podpis majitele soukromého klíče (N,d) pod zprávu M, aniž bychom potřebovali získat přístup k jeho klíči - datům na vytvoření podpisu.

Celá myšlenka je založena na tom, že RSA je distributivní vzhledem k násobení, protože platí: $\forall a,b \in Z , k \in N : (ab)^k \equiv a^k b^k \bmod N$.

Postup

Mějme zprávu M, ke které chceme získat podpis nějaké osoby (Boba), tj. hodnotu $M^d \bmod N$. Bobovi předložíme místo vlastní hodnoty M , kterou by Bob mohl z pochopitelných důvodů odmítnout podepsat, (zdánlivě) náhodnou hodnotu X. Tuto hodnotu X však předem pečlivě připravíme a to jako $M\ c^e \bmod N$. Zde c je náhodně zvolená veličina, (N,e) veřejný klíč Boba, M zpráva. Pokud Bob takovýto zdánlivě „nesmyslny“ text podepíše a my se k výsledku dostaneme, pak jsme schopni poměrně jednoduše vypočítat podpis Boba pro zprávu M.

Vše si ukážeme na konkrétním příkladě:

Nechť Bob má veřejný klíč (3337,79). Tedy modul N je 3337 a veřejný exponent je 79. Pozorní čtenáři si jistě všimli, že tyto parametry byly použity i v doprovodném příkladě úlohy z Crypto-Worldu 11/2001. Pro tato čísla jsme vypočetli hodnotu tajného-soukromého exponentu d=1019. Vypočítat soukromý exponent se nám podařilo proto, že byla použita

"malá" prvočísla. V tomto případě ale není podstatné, zda lze provést faktorizaci. Útok lze realizovat i pro skutečné klíče. Tedy v případě, kdy nelze pro výpočetní složitost soukromý exponent d vypočítat. V takovém případě si stačí naimplementovat aritmetiku velkých čísel a postupovat dále podle tohoto návodu.

Chceme získat Bobův podpis pod zprávu M=DLUH JE 10 USD

Nejprve si převedeme pomocí kódové tabulky text zprávy M do číselné posloupnosti .
M= D L U H J E 1 0 U S D
M= 68 76 85 72 61 74 69 61 91 60 61 85 83 68

M dále zformátujeme podle pravidla Crypto#1.12 na bloky m_1 m_2 m_3 …..
M = m_1 m_2 m_3 ….. = 0687 0685 0726 0174 0696 0191 0606 0185 0836 0800

Předpokládejme, že Bob má k dispozici program / prohlížeč, který by mu tuto zprávu zobrazil jako : DLUH JE 10 USD

Takovouto zprávu by pravděpodobně odmítl podepsat. Z tohoto důvodu připravíme zprávu jinou.

Zvolíme nějaké libovolné číslo c, např. 105 a dále spočteme číslo $x \equiv c^e \bmod N$.
Pro konkrétní hodnoty Bobova veřejného klíče dostaneme $x \equiv 105^{79} \bmod 3337 \equiv 193$.
Nyní připravíme k podpisu (zdánlivě) náhodnou nic nevyjadřující hodnotu $M\,c^e \bmod N$.

Pro naše konkrétní hodnoty spočteme:
M = m_1 m_2 m_3 ….. = 687 685 726 174 696 191 606 185 836 800
$M\,c^e \bmod N$ = $m_1\,c^e \bmod N$ $m_2\,c^e \bmod N$ $m_3\,c^e \bmod N$ ….. =
687*193 mod 3337 685*193 mod 3337 726*193 mod 3337 …..

M	0687	0685	0726	0174	696	0191	0606	0185	0836	800
$M\,c^e \bmod N$	2448	2062	3301	0212	848	0156	0163	2335	1172	898

Pro konkrétní výpočet lze např. použít program RSAM, který lze najít na domovské stránce Crypto-Worldu (příloha k e-zinu 11/2001). Nebo programy, které jste si vytvořili pro potřeby řešení úlohy z minulého čísla.

Bob nyní svým prohlížečem vidí text, který nemá žádný smysl. Nyní jej požádáme o podpis (např. „aby nám ukázal jak se vlastně dá nějaký text elektronicky podepsat...“). Po ukázce, jak se to dělá, jej pochválíme a text, včetně podpisu si „schováme“ na památku. Zdá se vám to jako utopie? Myslíte si, že to není Bob, ale Blb? Udělal jsem malý pokus. Při výuce – jak podepisovat přílohu Microsoft Outlooku jsem požádal své žáky v učebně, aby jako přílohu použili např. „náhodný“ text, který jsem pro tuto lekci připravil na sdílený disk.
Dokonce jsem zdůraznil, že je to v jejich zájmu, neboť zde nikde nezůstane jimi podepsaný nějaký "smysluplný" text. Z deseti žáků všech deset pilně do svého e-mailu tento text jako přílohu vložilo a v rámci výuky e-mail s přílohu podepsalo a následně mi podepsaný text zaslalo. Příloha byl otisk textu „Podepíši cokoliv“. Jistě lze najít další situace, kdy podpis Boba pod námi připravený text pod nějakou záminkou vymámíme a k výsledku se následně dostaneme.

Vraťme se k našemu příkladu. Text, který jsme připravili, je tento:
$M\ c^e \bmod N$ 2448 2062 3301 0212 848 0156 0163 2335 1172 898

Nyní jej předložíme Bobovi k podpisu. Ten vidí nesmyslný obsah a text proto klidně podepíše. Bob spočte $(M*c^e)^d \bmod N$ a dostane:
0310 1359 0031 2697 880 3048 1195 1229 0821 2502

Nyní použijeme trochu matematiky (řada kroků je vynechána nebo jen naznačena):
$(M\ c^e \bmod N)^d \bmod N \equiv M^d * c^{ed} \bmod N \equiv M^d * c \bmod N$ (využito $e*d \equiv 1 \bmod N$)
Výsledek lze zapsat jako $M^d * c \bmod N$.

Pokud se k tomuto podpisu dostaneme, lze ze znalosti hodnoty $M^d * c \bmod N$ a hodnoty C vypočítat podpis zprávy M tj. hodnotu $X \equiv M^d \bmod N$

K tomu potřebujeme postupně řešit následující soustavu modulárních rovnic:
$0310 \equiv 105 * M^d \bmod 3337$
$1359 \equiv 105 * M^d \bmod 3337$
$0031 \equiv 105 * M^d \bmod 3337$
$2697 \equiv 105 * M^d \bmod 3337$
....
$2502 \equiv 105 * M^d \bmod 3337$

Jejich vyřešením dostaneme následující hodnoty. Označíme je jako posloupnost (*).
1592 0585 1494 3172 644 3080 0647 1855 0707 1740
(K řešení těchto rovnic je potřeba napsat krátký program. Lze poměrně snadno realizovat i pro velká čísla.)

Malá nápověda

```
Procedure Solution;
Begin
writeln('Reseni modularni rovnice A=C*X mod N pro ruzna A');
        j:=0; M:=1;
    repeat
        inc(j);
        M1:=C*j-A;
        if M1>0 then
        begin
            M2:=((c*j-A) div N)*N;
            M:=M1-M2;
        end;
    until M=0;
    writeln('A=C*X mod N, X=',j);
end;
```

Posloupnost (*) je Bobův podpis zprávy M = DLUH JE 10 USD.

Našli jsme tedy postup, jak ke zprávě M získat podpis a to bez toho, že by Bob zprávu podepsal, a výpočet jsme provedli bez znalosti Bobova soukromého klíče (dat na vytvoření podpisu).

Na závěr ještě ověříme, že se skutečně jedná o Bobův podpis datové zprávy M (podle našeho podpisového schématu).

Zpráva M:
D L U H J E 1 0 U S D

Zpráva po převodu do číselného kódu:
68 76 85 72 61 74 69 61 91 60 61 85 83 68

Zpráva po formátování podle Crypto#1.12:
0687 0685 0726 0174 0696 0191 0606 0185 0836 0800

Nyní tuto zprávu podepíšeme pomocí Bobova soukromého klíče d (tj. spočteme M^d mod N, pro N=3337, d=1019) a dostaneme:
1592 0585 1494 3172 644 3080 0647 1855 0707 1740

Vidíme, že výsledek je shodný s posloupností (*). Tím jsme dokázali, že Bobův podpis zprávy M je skutečně shodný s posloupností, kterou jsme získali výše popsaným způsobem.

Úloha č.6 - Elektronický podpis

Vaším úkolem je získat Bobův podpis k tomuto textu (bez toho, že dopočítáte soukromý klíč) : M = SOUHLASIM S ROZVODEM
Bobův veřejný klíč je (modul, e) = (2479, 101)
(10 bodů za zaslání podpisu pod tento text)

Nápověda :
1) převodová kódová tabulka je shodná s tabulkou v předchozím cvičném případě
2) formátování použijte podle námi zavedeného standardu Crypto #1.12
3) pro výpočet "velkými čísly" lze použít program **RSAM** (9 kB) ("Repeated Squaring Method")

Úloha č.7 - Záchyt

Poslední úlohou je zjistit obsah zprávy, kterou se vám podařilo zachytit (soubor uloha7.wav) !
(10 bodů za zaslání obsahu zprávy)

Nápověda:
1) ti kteří vyřešili všechny předchozí úlohy - nápovědu nepotřebují
2) ostatní by měli začít řešením úkolů prvního kola ☺

Závěrečné pokyny pro řešitele
Řešení zašlete e-mailem na adresu pavel.vondruska@post.cz (kopii prosím zaslat na vondruska.p@seznam.cz a na pavel.vondruska@uoou.cz). Předmět označte heslem : ULOHA-6, 7
Termín: do slosování budou zařazena všechna správná a úplná řešení, přijatá do **30.12.2001** !

B. Kryptografie a normy - Díl 11. Digitální certifikáty
Část 3. Norma X.509, verze 4.
Jaroslav Pinkava, AEC spol. s r.o.

l. Úvod

V roce 2000 byla vydána nová verze normy X.509 s pořadovým číslem 4 (i jako nová verze normy ISO/IEC International Standard 9594-8). Jejím cílem (v návaznosti na jejího předchůdce - normu X.509 verze 3) je definice rámce pro práci s certifikáty veřejných klíčů, s atributovými certifikáty a autentizační služby.

2. Co je nového v normě X.509 - verze 4?

Daný dokument dává rámec pro práci v PKI (Public-Key Infrastructure) a dále v tzv. PMI (Privilege Management Infrastructure). Smyslem pojmu PMI je přitom formování modelu práce s různými typy oprávnění.

Tento rámec zahrnuje modely infrastruktur obou typů, definice syntaxe certifikátů a CRL, definice adresářových schémat a procedury pro vyhodnocování cest. Cílem je vytvořit formát digitálních certifikátů a CRL, který by byl dostatečně flexibilní, tj. vyhověl by potřebám všech potenciálních skupin uživatelů.

Nová struktura dokumentu obsahuje tři základní oddíly (viz příloha):
- certifikáty veřejných klíčů;
- atributové certifikáty;
- použití X.500 adresářů pro certifikáty veřejných klíčů a atributové certifikáty.

Základní model (z verze 3) zůstal nedotčen. Byly rozšířeny možnosti formátů digitálních certifikátů a CRL (zůstaly však zpětně kompatibilní). Mechanizmus práce s rozšířeními nyní umožňuje zavést doplňky pro specifické potřeby aplikací.

Verze 3 obsahoval pouze základní syntaxi atributových certifikátů (v1). Verze 4 normy X.509 obsahuje rozšířenou syntaxi atributových certifikátů (v2), definuje model PMI, specifikuje procesy pro ověřování cest při delegaci pravomocí, standardní množinu PMI rozšíření a příslušné adresářové schéma.

Verze 2 atributových certifikátů umožňuje užší provázání na autentizační certifikáty a také ale umožňuje objektům bez certifikátu veřejného klíče mohou vydávat atributové certifikáty. Verze (v2) atributových certifikátů je zpětně kompatibilní s verzí 1.

Došlo (z hlediska verze 3) k následujícím doplňkům v obsahu dokumentu:
- přidání nových rozšíření;
- doplnění schématu pro adresáře;
- jasnější popis delta CRL;
- definice modelu PMI + přidání rozšíření + adresářové schéma + definice pravidel pro zpracování privilegií.

Čeho se tyto úpravy týkají? Následují některé podrobnosti (samozřejmě pro čtenáře, který se zajímá o hlubší detaily, je nezbytné obrátit se na samotný dokument mající více než 150 stran).

Nová rozšíření:
- OID je definováno pro obecnou hodnotu v rozšíření certificatePolicies;
- přidáno rozšíření inhibitAnyPolicy;
- freshestCRL rozšíření umožňuje odkazy na delta CRL;
- deltaInfo rozšíření umožňuje nasměrovat dostupná delta CRL;
- nová CRL rozšíření (crlScope, orderedList, crlStreamIdentifier, statusReferrals, baseUpdateTime)

Adresářové schéma:
- nahrazující třídy objektů (pkiUser, pkiCA);

Nové definice objektů PKI:
- deltaCRl, cpCps, pkiCertPath;

Doplňky pro delta CRL:
- práce v čase, přístupnost

Cesta pro ověření certifikátu:
- některé opravy a modifikace

Další změny:
- certifikáty, kterým vypršela jejich platnost mohou být v CRL;
- CA nemusí mít jediné úplné CRL.

Řízení privilegií:
- obdoba modelů PMI a PKI;
- rozšířená syntax atributových certifikátů;
- definice rozšíření certifikátů.

Vzhledem k tomu, že norma poskytuje rámec pro fungování dvou modelů PMI a PKI, je užitečné mít na zřeteli některé základní analogické prvky obou modelů:

Entita PMI	**Entita PKI**
Zdroj autority (SOA)	kořenová CA
Atributová autorita (AA)	certifikační autorita (CA)
Držitel privilegie (oprávnění)	majitel certifikátu
Ověřovatel oprávnění	spoléhající se (ověřující) strana

3. Shrnutí

Ve stručném přehledu novinek verze 4 normy X.509 bylo možné ukázat pouze nejdůležitější změny dokumentu. Problematika se bude vyvíjet i nadále, např. další možné

zásahy do normy X.509 mohou přinést vznikající požadavky v rámci vývoje norem pro WAP (bezdrát). Na druhou stranu většina dnešních aplikací stále ještě pracuje s verzí 3 spíše než s verzí 4.

Některé pojmy:
Atributový certifikát: Datová struktura digitálně podepsaná atributovou autoritou, která propojuje některé hodnoty atributů s informacemi o identifikaci jejich držitele.
Atributová Autorita (AA): Autorita, která přiřazuje oprávnění vydáváním atributových certifikátů.
delta-CRL (dCRL): Částečný seznam odvolaných certifikátů, který obsahuje pouze ta data, která změnila svůj revokační status vzhledem k základnímu (base) CRL.
base CRL: CRL, které je použito jako základ při vytváření dCRL.
full CRL: Úplný seznam odvolaných certifikátů.
oprávnění: Atribut či vlastnost, která je entitě přiřazena autoritou.

4. Literatura

[1] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8: "INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY: PUBLIC-KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS", Version 4, 2000

5. Příloha (z obsahu normy)

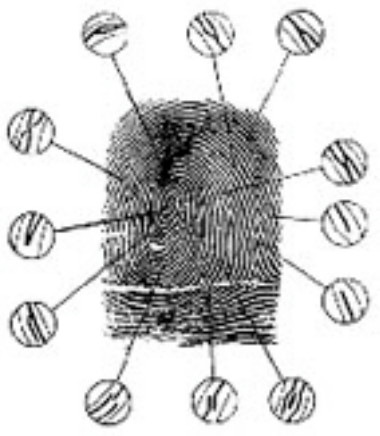
SECTION 1 - GENERAL
SECTION 2 - PUBLIC-KEY CERTIFICATE FRAMEWORK
7 Public-keys and public-key certificates
8 Public-key certificate and CRL extensions
9 Delta CRL relationship to base
10 Certification path processing procedure
11 PKI directory schema
SECTION 3 - ATTRIBUTE CERTIFICATE FRAMEWORK
12 Attribute Certificates
13 Attribute Authority, SOA and Certification Authority relationship
14 PMI models
15 Privilege management certificate extensions
16 Privilege path processing procedure
17 PMI directory schema
SECTION 4 - Directory use of public-key & attribute certificate frameworks
18 Directory authentication
19 Access control
20 Protection of Directory operations
Annex A Authentication Framework in ASN.1
Annex B CRL Generation and Processing Rules
Annex C Examples of Delta CRL Issuance
Annex D Privilege Policy and Privilege Attribute Definition Examples
Annex E An introduction to public key cryptography
Annex F Reference definition of algorithm object identifiers
Annex G Examples of use of certification path constraints
Annex H Alphabetical list of information item definitions
Annex I Amendments and corrigenda

C. Asyřané a výhradní kontrola

Radek Haubert, NKÚ

Identifikace pomocí otisků prstů je dnes patrně nejvíce používanou biometrickou metodou a to z několika důvodů, zejména její vysoké bezpečnosti, relativně nízké ceny a dobré dlouhodobé zkušenosti. Přestože o položení teoreticko - vědeckých základů daktyloskopie, jakožto základu pro identifikaci a pozdější autentizaci, se zasloužil anglický přírodovědec Francis Galton, když matematickými metodami vypočítal, že existuje celkem 64 miliardy různých variant v uspořádání papilárních linií a tím prakticky vyloučil možnost výskytu dvou jedinců se stejným obrazcem papilárních linií (výsledky své práce sdělil veřejnosti 25. května 1888), znalost daktyloskopie byla prokázána už u Asyřanů.. Otisky prstů se nacházejí i na výrobcích z keramiky, zvláště pak uměleckých kachličkách, nalezených při archeologických vykopávkách v Řecku, na území bývalého Římského impéria a v Egyptě. Prvním autorem spisku o otiscích prstů, jako prostředku ke zjišťování totožnosti osob, byl Číňan Kio Kung-yen. V Japonsku pochází první zmínka o daktyloskopii z roku 672 a byla uveřejněna v roce 720 v knize Dějiny Japonska "Nihongi". Otisk prstu je v Japonsku uznáván prakticky ve stejný čas jako v Číně.[1] Významné místo v daktyloskopii zaujímá Juan Vucetich (1838-1925), jenž působil v Buenos Aires a je dokonce považován na tvůrce pojmu daktyloskopie. Jeho teoretická díla stejně jako jeho daktyloskopický klasifikační a subklasifikační systém se rozšířily po celém světě.

Rozpoznávání otisků prstů můžeme rozdělit na *identifikační* mód, používaný v kriminalistice, kdy hledáme shodu mezi otiskem či jeho fragmentem a všemi otisky uloženými v databázi; příkladem takového systému je počítačový systém AFIS 2000 americké firmy Pintrac, jehož kapacita systému je 800.000 daktyloskopických karet a 20.000 daktyloskopických stop (používán od října 1994 policií ČR) a na *ověřovací* mód, používaný v autentizačních systémech ke kontrole identity. Systém pak nezjišťuje shodu mezi nasnímaným vzorkem a celou databází, ale jen shodu mezi nasnímaným vzorkem a referenční šablonou, tedy biometrickými daty uloženými v biometrickém systému. Dalším rozdílem mezi oběma módy jsou samotná ukládaná data, v identifikačních systémech jsou ukládány celé otisky, zatímco v systémech určených pro autentizaci jsou ukládány pouze údaje o identifikačních bodech, které postačují k rozhodnutí, zda je či není nasnímaný otisk shodný, ale nelze z nich zpětně rekonstruovat otisk jako takový.



Identifikační body tvoří zvláštnosti (tzv. markanty – viz. obrázek vpravo) papilárních linií (háček, vidlice, očko, zkřížení, můstek a pod.). Papilární linie jsou kožní lišty na prstech, dlani a plosce nohy u člověka a opic. Vznikají při soustavném uchopování předmětů i na kůži amputačních pahýlů končetin (tzv. Bartošův fenomén), a jsou přítomny i na kontaktní straně chápavých ocasů opic. Odvozují se od konfigurace škáry a pokožky, jejich podkladem jsou tzv. hmatové podušky. Otisk prstu obsahuje v průměru až 175 identifikačních bodů.

Snímače lze rozdělit podle použité technologie na optické, kapacitní, ultrazvukové atd. Činnost autentizačního systému znázorňují následující obrázky získané z aplikace PassPrint Demo verze 2.5 určené pro otestování otisků prstů za

[1] JEDLIČKA, Miroslav. *Kriminalistická daktyloskopie* [online]. Dostupný z: <http://www.spsmvbr.cz/Os_stranky/jedlicka/daktyl/daktyl.htm>.

použití kapacitního snímače 5thSence od firmy Veridicom. Vlevo jsou umístěny otisky před zpracováním, vpravo pak po něm s vyznačenými identifikačními body. Slaběji zobrazené body představují ukončení papilární linie, silněji zobrazené body rozdvojení papilární linie.

Po sejmutí otisků se porovnávací algoritmus musí vyrovnat nejen s rozdílnou kvalitou otisků, rozdílným počtem nalezených identifikačních bodů, ale i s posunutím ve všech směrech a pootočením až o několik stupňů. Například z první dvojice obrázků představujících data pro referenční šablonu systém získal 37 identifikačních bodů, zatímco na druhé dvojici obrázků představující ověřovaný otisk je 41 identifikačních bodů, ale společných bodů mají oba vzorky „jen“ 22. Vzorky jsou oproti sobě posunuty na vodorovné ose o 3 body, na svislé ose o 16 bodů a pootočeny o 4,61 stupně. Tato shoda je však dostatečná a algoritmus vyhodnotí oba vzorky jako patřící jedné osobě.

Udávané parametry se v různé literatuře liší, závisí jak na snímači tak na použitém algoritmu a přibližně činí:

- pravděpodobnost chybného odmítnutí (FRR): <1.0%
- pravděpodobnost chybného přijetí (FAR): od 0.0001% do 0.00001% podle typu
- čas ověření: 0.2 až 1 sekunda.

Tyto postupy se v současné době již používají na mnoha místech a různých oborech. Jedním z příkladů je systém sociálního zabezpečení, provozovaný v části Los Angeles, používající automatické vyhledávání otisků prstů jako ochrany před zneužíváním sociálních dávek formou jejich vícenásobného uplatňování. Tato služba má být rozšířena i do dalších států USA. Podobně transakce pro vyplácení důchodů První národní banky v Jižní Africe, která má 48 000 klientů, vyžaduje ověření otisků prstů.

Výhody této metody autentizace spočívají především v nízké ceně (od 150 amerických dolarů za snímač), rychlosti, přesnosti a jednoduchosti použití. Pro použití hovoří celá škála různých typů snímačů od rozměrných, sloužících většinou k přístupu do budov či místností, až po provedení PC Card přinášející vysoké zabezpečení s využitím otisku prstu také do

oblasti přenosných počítačů a notebooků. Celý snímač je zabudován do PC karty (PCMCIA) typu II. Pro identifikaci jednoduše stisknete boční část karty, z karty se vysune snímací část a na ni můžete přiložit prst.

V blízké budoucnosti budou kapacitní snímače integrovány do čipových karet a to buď jako další bezpečnostní prvek, nebo jako náhrada PINu. Použití takové karty by podle mého názoru, bylo mimořádně vhodné pro uchovávání privátního klíče, protože s velkou mírou jistoty zaručuje jednu ze základních podmínek ZoEP a to že „byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou“.

Nevýhody pak představuje především závislost výsledku na kvalitě vzorku, jenž ovlivňuje zejména míra nečistot ulpívajících na snímači. Dalším problémem nebývají jak by se mohlo zdát větší poranění prstů, ale naopak drobná ovšem často se opakující poškození papilárních linií, způsobených obvykle manuální činností. Nemusí se vždy jednat o těžkou fyzickou práci, jako jsou hornické či zednické práce, obyčejné časté mytí nádobí za použití dnes velmi agresivních čistících prostředků může způsobit, že při autentizaci je otisk požadován místo obvyklé sekundy stále znovu a znovu i několik minut, než se jej podaří sejmout v kvalitě odpovídající požadované bezpečnostní úrovni, nebo se to nepodaří vůbec. Podle mých zkušeností s konkrétní implementací se počet uživatelů, jenž pro své mimořádně nečitelné otisky nejsou schopni tuto technologii využívat, pohybuje okolo 3 procent.

D. Jak se (ne)spoléhat na elektronický podpis

Bc. Jan Hobza, ÚOOÚ, jan.hobza@uoou.cz

Všichni již víme, že elektronický podpis je jedinečné číslo, které vytváří podepisující osoba pomocí svých dat na vytváření elektronického podpisu a zprávy, kterou podepisuje. Data na vytváření elektronického podpisu (dále jen soukromý klíč) se generují spolu s daty pro ověřování elektronického podpisu (dále jen veřejný klíč) pouze jednou za životní cyklus certifikátu a pro bezpečnost celého systému je jejich bezpečné uchovávání velice důležité. Veřejný klíč je naopak informace, kterou může mít k dispozici neomezený počet osob a bezpečnost používání elektronického podpisu tím není nijak ohrožena. Při samotném vytváření elektronického podpisu aplikuje podepisující osoba svůj soukromý klíč na danou zprávu a tento dokument spolu s elektronickým podpisem a certifikátem odesílá spoléhající se straně (např. příjemci pošty). Podle zákona o elektronickém podpisu musí podepisující osoba mimo jiné dbát na to, aby její soukromý klíč nemohl být neoprávněně zneužit a chránit ho proti takovému zneužití. Za porušení této povinnosti podepisující osoba odpovídá podle občanského zákoníku. Příjemce zprávy pak běžným způsobem ověří platnost elektronického podpisu a to ‚zda certifikát, který je nositelem veřejného klíče podepisující osoby, nebyl zneplatněn. Pokud je vše v pořádku, spoléhající strana se může na tento podpis spolehnout.

Z uvedených řádků se může zdát, že spoléhající se strana hraje v celém procesu užívání elektronického podpisu poněkud pasivní roly: certifikační autorita (po provedení patřičných úkonů) vytvoří pro podepisující osobu certifikát k datům na ověření elektronického podpisu, podepisující osoba pak elektronicky podepíše určitá data a spoléhající se stana pouze ověří platnost a buď se spolehne na podpis či ne. Ve skutečnosti je tomu jinak.

Celý proces, jak jsme si ho výše nastínily, je založen na tom, že spoléhající se strana je ochotna náš certifikát přijímat. V žádném právním předpisu se nestanoví povinnost spoléhající se strany přijímat a spoléhat se na jakýkoli certifikát, byť platný a kvalifikovaný. Asi málo z nás by otevřelo elektronicky podepsaný spustitelný soubor u něhož by byl přiložen certifikát se jménem Mickey Mouse. Předpokladem úspěšné elektronické komunikace tedy musí ***být vůle a souhlas druhé strany k této komunikaci.*** Co z toho vyplývá?

Je to právě spoléhající se strana, která si může diktovat, jak má daný certifikát vypadat (které další dispozitivní atributy má obsahovat, zda musí nést jméno podepisující strany, či stačí pouze její pseudonym apod.). Je to spoléhající se strana, která určí, jakým způsobem bude ověřovat statut zneplatnění certifikátu (CRL, OCSP, DeltaCRL apod.) a v jakých intervalech tak bude činit. A především je to spoléhající se strana, která rozhodne, jaké certifikáty a od jakého poskytovatele bude přijímat a jakou míru zabezpečení bude požadovat. Důkazem toho nám budiž zahraniční praxe.

Nejdále v používání elektronického podpisu a zároveň nejblíže v principech zákona o elektronickém podpisu nám je jistě Německá spolková republika. Elektronický podpis je zde uzákoněn již od roku 1997 a od této doby se v Německu akreditovalo 16 poskytovatelů certifikačních služeb. Každý z nich vydává různé kvalifikované certifikáty pro různé agendy. Jedině tak mohou uspokojit různorodou poptávku trhu a zároveň se na něm udržet. Období, kdy převládala poptávka po „jakýchkoli“ certifikátech vydaných na základě zákona (tak, jak to nyní zažíváme i u nás), brzy vystřídal její pokles a po čase byli poskytovatelé certifikačních služeb nuceni nabízet takové certifikáty, které přesně odpovídají požadavkům jednotlivých agend (advokátní komora, zdravotnické odbory, telekomunikační společnosti a v neposlední řadě orgány veřejné správy).

Způsob, jakým toho lze dosáhnout je v zásadě velice jednoduchý. Subjekty, které spolu chtějí komunikovat v rámci zákona a s použitím elektronického podpisu, a zároveň mají zvláštní požadavky na tuto komunikaci, se dohodnou s vybranou certifikační autoritou na struktuře poskytovaných služeb a samozřejmě na jejich ceně. Certifikační autorita pak vytvoří odpovídající Certifikační politiku (případně i novou Certifikační prováděcí směrnici), podle které bude dané služby poskytovat. Certifikační autorita dále ověří u příslušného akreditačního orgánu (v případě české republiky je to Úřad pro ochranu osobních údajů), zda tyto služby (a samozřejmě jejich realizace) splňují požadavky zákona. Dalším krokem je již poskytování těchto certifikačních služeb.

Nic nebrání tomu, aby se podobné procesy rozeběhly i v České republice. Je naprosto zřejmé, že kvalifikovaný certifikát, tak jak ho definuje zákon o elektronickém podpisu, a revokační služba (služba zneplatnění certifikátů) s 12ti hodinovou lhůtou na zveřejnění, nebudou dostatečné pro potřeby veškerých komunikačních agend ani u nás. Zda bude všem orgánů veřejné moci při vyřizování podání postačovat, že přiložený certifikát je kvalifikovaný, je spíše nepravděpodobné. Ani zákon ani jiný podzákonný předpis však nemohou klást další požadavky na poskytovatele certifikačních služeb potažmo na jejich služby, neboť by to odporovalo článku 3 Směrnice 1999/93 ES, která byla jejich výchozím bodem. Je tedy na jednotlivých orgánech veřejné moci a samozřejmě na dalších subjektech, které chtějí využívat elektronický podpis v rámci zákona, aby stanovily své požadavky a prosadily je poskytovatelů certifikačních služeb.

E. Některé odlišnosti mezi českým zákonem 227/2000 Sb. (Zákon o elektronickém podpisu a o změně některých dalších zákonů) a poslaneckým návrhem obdobného zákona na Slovensku.

RNDr. Dagmar Brechlerová, KIT PEF ČZU, brechlerova@pef.czu.cz

Následující článek se snaží poukázat na některé odlišnosti českého zákona a slovenského návrhu zákona. Vzhledem k rozsahu textu není samozřejmě poukázáno na veškeré rozdíly, pouze na ty, které autorku článku nejvíce zaujaly. Rovněž tak zde není diskutována problematika navazujících změn v dalších zákonech.

Český zákon byl přijat 29. 6. 2000, jeho účinnost nastala od 1. 10. 2000. Plné znění zákona lze najít ve sbírce zákonů nebo např. na [2]. Na Slovensku se jedná zatím o návrh zákona, na kterém pracovala skupina odborníků z různých oblastí vedená docentem Olejárem z MFF UK Bratislava, složení celé skupiny a současné znění návrhu zákona možno najít na [1]. Na stejné adrese je možno najít důvodovou zprávu, která velmi dobře vysvětluje pojmy z problematiky elektronického podpisu. Návrh slovenského zákona zatím prošel dvěma čteními slovenského parlamentu a je, pokud je nám známo, velká šance na přijetí. Nepochybně může před konečným schválením zákona dojít ještě ke změnám.

Jaký je mezi texty rozdíl či lépe rozdíly? Je jich celá řada a tento článek upozorňuje na některé z nich.

První rozdíl je již v délce zákona, slovenský návrh má nejen více paragrafů, ale i délka textu je více než o polovinu delší. Z toho plyne, že řada termínů je podrobněji v slovenském návrhu specifikována a vysvětlena. Partie ze slovenského textu budou dále citovány v originále, čtenářům to jistě nebude dělat potíže. Části zákonů jsou psány kurzívou.

Další rozdíl je již v tom, co se vlastně podepisuje. V České republice je to **datová zpráva**, v českém zákoně je následující část

§ 2… Vymezení některých pojmů
Pro účely tohoto zákona se rozumí
c) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou

ve slovenském návrhu je popsaný **dokument, digitální dokument a elektronický dokument,** podepisuje se **elektronický dokument.**

§ 3 1.
Na účely tohto zákona sa rozumie: pod dokumentom ľubovoľná konečná neprázdna postupnosť znakov. Pod digitálnym dokumentom sa rozumie digitálne (číselne) kódovaný dokument. Pod elektronickým dokumentom sa rozumie digitálny dokument uchovávaný na fyzickom nosiči; prenášaný alebo spracovávaný pomocou technických prostriedkov v elektrickej, magnetickej, optickej alebo inej forme.

Další odlišnost a to dle našeho názoru velmi závažná je v užívání elektronického podpisu v kontaktu s veřejnou správou. Slovenský návrh toto řeší paragrafem 6, který říká

§ 6
Používanie elektronického podpisu

1. *Elektronický podpis sa môže používať bez obmedzenia, ak všeobecne záväzný právny predpis neustanovuje inak.*
2. *Ak je v styku s verejnou správou možné používať elektronický podpis, tak tento elektronický podpis musí spĺňať podmienky podľa § 5 tohto zákona.*

V §5 je poté podrobně popsán Zaručený elektronický podpis. Jak výše uvedeno, je zde výraz "ve styku s veřejnou správou", zatímco v českém zákoně je velmi často diskutovaný problematický §11:

§ 11
V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

Zde je některými právníky upozorněno na nejasnost pojmu :"V oblasti orgánů veřejné moci".

Co v českém zákoně oproti slovenskému návrhu zcela chybí, je jakákoliv zmínka o časových potvrzeních. Ve slovenském návrhu je této problematice věnován celý paragraf 11, který je natolik zajímavý, že ho zde ocitujeme celý.

§ 11
Časová pečiatka

1. *Časová pečiatka je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá spĺňa nasledujúce požiadavky:*
    a. *nie je (efektívne) možné ju vytvoriť bez znalosti súkromného kľúča určeného na tento účel,*
    b. *na základe znalosti verejného kľúča prislúchajúceho k súkromnému kľúču použitému pri jej vytvorení je možné overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, nebol po jej vytvorení zmenený,*
    c. *je vytvorená akreditovanou certifikačnou autoritou použitím súkromného kľúča určeného na tento účel,*
    d. *je možné ju vytvoriť len s použitím bezpečného zariadenia na vytváranie časovej pečiatky podľa §3, ods. (23),*
    e. *na verejný kľúč prislúchajúci k súkromnému kľúču použitému na jej vytvorenie bol akreditovanou certifikačnou autoritou vydaný kvalifikovaný certifikát,*
    f. *umožňuje jednoznačne identifikovať dátum a čas, kedy bola vytvorená.*
2. *Formát časovej pečiatky a spôsob jej vytvárania, požiadavky na zdroj časových údajov pre časovú pečiatku a požiadavky na vedenie dokumentácie časových pečiatok ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.*

Tato problematika v českém zákoně nijak řešena není.

Další významný rozdíl mezi českým zákonem a slovenským návrhem je v tom, kdo je pověřen akreditací poskytovatelů **certifikačních služeb** a dozorem nad nimi. V České republice to je **Úřad pro ochranu osobních údajů**. V paragrafu 6 je zavedeno, kdo je „Úřad" a dále je celý § 9 věnován vysvětlení, co všechno Úřad dělá.

§ 6

……j) používat bezpečné systémy a nástroje elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují; nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou; toto musí být ověřeno ***Úřadem pro ochranu osobních údajů (dále jen "Úřad"),***

§ 9 *Akreditace a dozor*

(1) Udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb, jakož i dozor nad dodržováním tohoto zákona náleží Úřadu.

…….

Na Slovensku mají také v návrhu Úřad , zde to je však „**Úrad pre elektronický podpis**“, který má být součástí NBÚ.

§ 2

Účel zákona

.....

e. Účelom zákona je: upraviť postavenie a pôsobnosť orgánu štátnej správy, ***Úradu pre elektronický podpis*** *(ďalej len Úrad) pri vykonávaní certifikačných činností,*

§ 12

Úrad

1. Zriaďuje sa ***Úrad pre elektronický podpis*** *ako súčasť Národného bezpečnostného úradu podľa § 34, ods. (1) tohto zákona.*

Je samozřejmě otázkou, pokud tato část textu zůstane na Slovensku v konečném znění zákona, které řešení se ukáže jako lepší.

V České republice zákon zná pouze **poskytovatele certifikačních služeb a akreditovaného poskytovatele certifikačních služeb**, na Slovensku kromě **certifikačních autorit** návrh zákona také zavádí pojem **registrační autorita**

§ 3

16. pod certifikačnou autoritou poskytovateľ certifikačných služieb, ktorý spravuje certifikáty podľa § 3 ods. (12) zákona.

17. pod akreditovanou certifikačnou autoritou certifikačná autorita, ktorá poskytuje akreditované certifikačné služby v súlade s týmto zákonom a všeobecne záväznými predpismi vydanými Úradom, a ktorá má na poskytovanie týchto služieb akreditáciu Úradu.

§ 3

18. pod registračnou autoritou poskytovateľ certifikačných služieb, ktorý v mene certifikačnej autority vykonáva vybrané certifikačné činnosti a sprostredkováva služby certifikačnej autority držiteľom certifikátov a žiadateľom o vydanie certifikátu.

V §18 jsou dále vysvětlena práva a povinnosti registrační autority.

Registračná autorita

1. *Registračná autorita koná v mene certifikačnej autority a na základe uzatvorenej zmluvy.*
2. *Vykonávanie certifikačných činností registračnou autoritou v mene certifikačnej autority podľa tohto zákona nie je viazané na žiadne povolenie.*
3. *Registračná autorita je vo svojej činnosti viazaná certifikačným poriadkom certifikačnej autority v mene ktorej koná.*

I k uznávání zahraničních certifikátů řeší se oba texty staví dosti odlišně a to hlavně do budoucna. V Čechách:

§ 16
Uznávání zahraničních certifikátů
(1) Certifikát, který je vydán zahraničním poskytovatelem certifikačních služeb jako kvalifikovaný ve smyslu tohoto zákona, může být používán jako kvalifikovaný certifikát tehdy, je-li uznán poskytovatelem certifikačních služeb, který vydává kvalifikované certifikáty podle tohoto zákona, a za podmínky, že tento poskytovatel certifikačních služeb zaručí ve stejném rozsahu jako u svých kvalifikovaných certifikátů správnost a platnost kvalifikovaného certifikátu vydaného v zahraničí.
(2) Certifikát, který je vydán zahraničním poskytovatelem certifikačních služeb jako kvalifikovaný ve smyslu tohoto zákona, je uznán jako kvalifikovaný certifikát tehdy, pokud to vyplývá z rozhodnutí Úřadu nebo mezinárodních smluv nebo pokud bude mezi příslušným zahraničním orgánem nebo zahraničním poskytovatelem certifikačních služeb a Úřadem uzavřena dohoda o vzájemném uznávání certifikátů.

Na Slovensku sice první část textu dosti odpovídá české verzi, ale slovenský návrh již dopředu řeší situaci po vstupu do Evropské unie.

§ 25
Uznávanie zahraničných certifikátov
(1) Certifikát, alebo kvalifikovaný certifikát, ktorý vydala certifikačná autorita so sídlom mimo územia Slovenskej republiky (zahraničná certifikačná autorita), ktorého platnosť možno overiť v Slovenskej republike, možno uznať v Slovenskej republike ak
- *a. zahraničná certifikačná autorita, ktorá ho vydala je akreditovaná v Slovenskej republike, alebo*
- *b. certifikačná autorita so sídlom v Slovenskej republike, ktorá spĺňa požiadavky zákona, garantuje platnosť certifikátu napr. vydaním krížového certifikátu verejného kľúča zahraničnej certifikačnej autority, alebo*
- *c. medzinárodná dohoda podpísaná Slovenskou republikou stanovuje, že (zahraničný) kvalifikovaný certifikát je uznávaný ako kvalifikovaný certifikát, alebo zahraničná certifikačná autorita je uznaná za akreditovanú certifikačnú autoritu v Slovenskej republike.*

(2) Dňom vstupu Slovenskej republiky do Európskej únie sa certifikát vydaný certifikačnou autoritou majúcou sídlo v niektorej z krajín Európskej únie, ktorého platnosť možno overiť v Slovenskej republike stáva rovnoprávnym certifikátu vydanému v Slovenskej republike. Kvalifikovaný certifikát vydaný vyššie uvedenou certifikačnou autoritou bude mať rovnakú právnu účinnosť ako kvalifikovaný certifikát vydaný v Slovenskej republike.

Navíc ve slovenském textu je řešena otázka křížových certifikací, které jsou pak např. v § 25 použity, v českém zákoně tato otázka vůbec řešena není.

Dalších rozdílů je velmi mnoho, doufáme, že se podařilo naznačit, že oba texty se v některých částech dosti liší. Na daném prostoru nebylo samozřejmě možno probrat všechny odlišnosti. Uvidíme, kdy a v jaké verzi bude schválen slovenský zákon, jaké poté budou prováděcí vyhlášky a jak se celá situace s elektronickým podpisem na Slovensku vyvine, nakolik bude stejná jako v Čechách a nakolik odlišná. Zájemcům o danou problematiku lze jak návrh slovenského zákona tak důvodovou zprávu jenom doporučit k prostudování, obojí je velmi zajímavé.

Literatura:
[1] http://www.informatika.sk/e-podpis
[2] http://www.uoou.cz

F. Letem šifrovým světem

Mikulášská kryptobesídka skončila.

Ve dnech 10.-11.prosince se konala v moderních prostorách jednoho ze sponzorů (SAP) Mikulášská kryptobesídka. Jednalo se o vydařenou mezinárodní akci, která proběhla v příjemném prostředí, klidné atmosféře a díky práci organizátorů bez problémů. Sešlo se zde na sedmdesát českých a slovenských odborníků a zvaní hosté Julien Marcil (RSA Security, UK) Fabien Petitcolas (Microsoft Research Cambridge, UK) a Bart Preneel (Katholieke Universiteit Leuven, Belgium). Program (včetně příspěvků) můžete najít na adrese http://www.ecom-monitor.com/kryptobesidka/index.html .

O nesplněných očekáváních v oblasti PKI, o tom jak stále chybí velké projekty a o problémech velkých PKI vendorů se v poslední době mluví stále více a více. Jeden z velice zajímavých článků na toto téma najdete na
http://www.infosecuritymag.com/articles/october01/columns_logoff.shtml

MPSV: Elektronický podpis nebude?! (11.12.2001, Svět Namodro)
Na tiskové konferenci MPSV v Telči, pořádané při příležitosti ukončení výstavby WAN systému státní sociální podpory, ředitel odboru informatiky MPSV Ing. Roman Kučera oznámil stop pro elektronický podpis. MPSV se tak rozhodlo z důvodu **legislativních vad zákona 227/2000 Sb. o elektronickém podpisu** (byl citován **paragraf 11** a Ing. Kučera jízlivě poznamenal, že na problém bylo upozorňováno již před přijetím zákona).
http://svet.namodro.cz/go/r-art.asp?id=1011210437&t=it

Kritikou zákona o elektronickém podpisu se zabývá i známý autor JUDr. Ján Matejka (Ústav pro stát a právo ČAV) http://www.lupa.cz/clanek.phtml?show=1974 .
Jeho článek "Zákon o e-podpisu obsahuje řadu legislativních chyb" byl publikován 12.12.2001 na serveru LUPA. Z obsáhlé kritiky vybírám : "Tento zákon totiž, nejenom že obsahuje řadu sporných ustanovení, která velmi zdržovala práce na prováděcích předpisech (zejména pak na vyhlášce), ale navíc se v něm objevuje stále více nedostatků, resp. nepříliš

vyhovujících ustanovení, která mohou v budoucnu vytvářet překážky jak v rámci e-commerce, tak i e-government... V řadě dalších aspektů (užívání v oblasti orgánů veřejné moci) pak elektronickou komunikaci téměř znemožňují. Velmi sporným a podstatným ustanovením této zákonné úpravy je problematický § 11. …"

O nejnovějším vývoji v oblasti kvantové kryptografie se můžete dočíst na
http://www.newscientist.com/news/news.jsp?id=ns99991595

Minulý měsíc byl neobyčejně bohatý na nové standardy a doporučení v oblasti kryptologie.

Největší událostí ve standardizační oblasti bylo bezesporu dlouho očekávané vydání nového šifrového standardu AES (Advenced Encryption Standard), který má postupně nahradit již zastaralý 3DES. Standard vydal 26.11.2001 NIST (National Institute of Standards and Technology) pod referenčním publikačním číslem FIPS-197.
AES : http://csrc.nist.gov/encryption/aes/
FIPS-197: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

NIST dále zveřejnil 66-ti stránkovou publikaci řady SP (Special Publication), která se zabývá módy blokových šifer (ECB, CBC, CFB, OFB a CTR). Plné referenční označení a název této zajímavé publikace je SP 800-38A, "Recommendation for Block Cipher Modes of Operation". Publikace vyšla 11.prosince.
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (225KB)
http://cryptome.org/bcm/sp800-38a.htm

NIST dále zveřejnil změnu ve známém dokumentu FIPS 186-2 "Digital Siganture Standard". Jedná se o 5-ti stránkový doplněk, který se týká náhodných generátorů. Tuto informaci naleznete na stránce věnované podpisovým schématům FIPS Cryptographic Toolkit (Digital Signatures) http://csrc.nist.gov/encryption/tkdigsigs.html . V současné době existují tři podle FIPS schválené (FIPS-approved*) algoritmy pro vytváření a ověřování digitálních podpisů (DSA, RSA a ECDSA) a jeden hashovací algoritmus SHA-1 . Informace a příslušné standardy FIPS naleznete na této přehledné stránce.

Na stránce NIST můžete najít i informace o právě skončeném listopadovém workshopu věnovanému správě klíčů (The Second Key Management Workshop).
Key-management : http://csrc.nist.gov/encryption/kms/

Možná, že si vzpomínáte na případ mladého Rusa Skljarova (ElcomSoft), který byl zadržen FBI 16.7.2001 na tradičním srazu hackerů v Las Vegas (Def Con). Psali jsme o něm na str. 22 v Crypto-Worldu 78/2001. Ruského programátora zatkla FBI za šíření demoverze programu ke čtení zabezpečených elektronických knih (konkrétně eBook Reader, produkt firmy Adobe). Pokračování tohoto případu můžete nalézt zde:
http://www.usdoj.gov/usao/can/press/html/2001_12_13_sklyarov.html
Mladý Rus podepsal, že bude spolupracovat na vyšetření celého případu. Byl propuštěn a může odcestovat zpět do vlasti.

Svět Namodro 13.12.2001 publikoval článek "Antivirové společnosti budou ignorovat virus vyvinutý FBI a používaný jako sledovací zařízení." Toto téma je v současné době komentováno na všech hlavních internetových zdrojích (zdnet, wired, theregister, cnet, excite…). O co vlastně jde? FBI zahájilo projekt nazvaný Magic Lantern (neboli magická lucerna), výsledek umožní vyšetřovatelům FBI vstoupit na "infikované" počítače a zde získat informace z klávesnice uživatele. Tyto informace jsou automaticky zasílány na adresu FBI a zde ukládány. Možné je tak například získat informace typu heslo, passphrase apod. a následně je využít k přístupu ke zdánlivě kvalitně zabezpečeným datům. Nejedná se o nic nového nebo nemožného. Podobných programů existuje a existovala celá řada. Připomeňme zde alespoň nechvalně známý program Back Orifice. Tvůrci však byli vždy hackeři (opravdu?). Co je však zcela nové, je prohlášení antivirových společností ve Spojených Státech. Rozhodly se detekci tohoto programu do svých softwarových balíků nezařadit!
http://svet.namodro.cz/go/r-art.asp?id=1011212524&t=security
http://www.zdnet.com/zdnn/stories/news/0,4586,5099906,00.html
http://www.theregister.co.uk/content/55/23150.html
http://news.excite.com/news/r/011212/18/tech-tech-magiclantern-dc
http://www.wired.com/news/conflict/0,2100,48648,00.html
http://www.theregister.co.uk/content/55/23057.html
http://news.cnet.com/news/0-1003-200-8134814.html

Již jste dostali "zábavnou SMS-ku", která vám zablokovala váš mobilní telefon? V poslední době se na toto téma objevilo několik zajímavých článků. Pokud se chcete dočíst o zranitelnosti mobilních telefonů řady Nokia, můžete se podívat na následující stránky:
http://www.theregister.co.uk/content/55/23080.html
http://www.theregister.co.uk/content/55/23232.html

O čem jsme psali v prosinci roku 1999 a 2000

Crypto-World 12/1999

Crypto-World 12/2000

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

G. 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.

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 jej najít na lépe dostupné adrese:

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**)

pavel.vondruska@post.cz

vondruska.p@seznam.cz