Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 78/2002 **5. srpen 2002**

78/2002

Připravil : Mgr.Pavel Vondruška

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

(351 e-mail výtisků)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Hackeři pomozte II. (poučný příběh se šťastným koncem)

Mgr. Pavel Vondruška, GCUCMP

V minulém čísle Crypto-Worldu (6/2002) jsme na straně 21 zveřejnili výzvu převzatou z Norway post - „Hackeři pomozte“, ve které se hledají osoby, které jsou schopny pomoci najít přístupové heslo do elektronického archívu norského muzea. Pracovník, který archív vytvořil a spravoval zemřel. Za svého života heslo nikomu nesdělil. Důležitá data v příslušné databázi se stala nedostupnými.

Problém se podařilo vyřešit a heslo bylo nalezeno. Pro některé poučné momenty celé kauzy se k tomuto příběhu ještě nyní vrátíme.

Všechno začalo před devíti roky – norské Centrum Ivara Aasena pro kulturu a jazyky začalo zpracovávat a převádět do digitální formy rozsáhlou sbírku obsahující více než 11 000 titulů a bibliografických materiálů, které shromáždil profesor Reidar Djupedal. Profesor se zabýval zrodem nového norského jazyka Nynorsk vycházejícího z místních dialektů. Jazyk aktivně používá okolo 20 procent obyvatel v západní části Norska a používá se běžně i v denním tisku. Zbytek obyvatel používá jazyk, který je kombinací dánštiny a staré norštiny. Jak jsme již psali, správce databáze informací o původním jazyku Nynorsk nedávno zemřel a přístupový kód k databázi nebyl nikde nalezen.

Když pracovníci muzea vyzkoušeli všechny jim dostupné prostředky a heslo nenašli, rozhodli se uveřejnit výzvu o pomoc na své internetové stránce. Tuto výzvu postupně převzala i různá další média. Pomoci mohl opravdu každý, neboť databáze byla zpřístupněna na webu muzea a kdo by našel správný přístupový kód, měl jej e-mailem zaslat zpět do Centra. Centru na základě výzvy pomohl programátor Joachim Eriksson. Tomu stačilo jen necelých pět hodin, aby heslo rozluštil. Data se tak opět stala přístupná pro historické a vědecké účely. Odhalené heslo „*ladepujd*“ ostatně nebylo zase tak velkým hlavolamem – je to jméno zakladatele a správce sbírky psané pozpátku….

Závěr :
- muzeum nemělo vhodnou bezpečnostní politiku, ve které by byl zajištěn přístup k datům v případě krizových situací
- heslo bylo vybráno nevhodně (odvoditelné, krátká délka, použita pouze písmena atd…)
- je otázkou, zda mělo smysl vůbec utajovat přístup k datům, když tato data byla nakonec volně vystavena na webu muzea a mohla být stažena libovolným zájemcem. Po zveřejnění hesla se údaje v databázi staly běžně dostupné.

Na základě zveřejněných informací se dá říci, že muzeum neprovedlo správné ocenění dat a nestanovilo příslušná bezpečnostní opatření související s ochranou dat podle zařazení do příslušné kategorie, nemá stanovenu politiku pro klíčové hospodářství, chybí kontrolní a dozorový mechanismus, chybí krizový plán resp. plán obnovy.

Není tak celý příběh poučením a také výzvou pro některé naše instituce a podniky?

B. Režimy činnosti kryptografických algoritmů

Mgr. Pavel Vondruška, GCUCMP

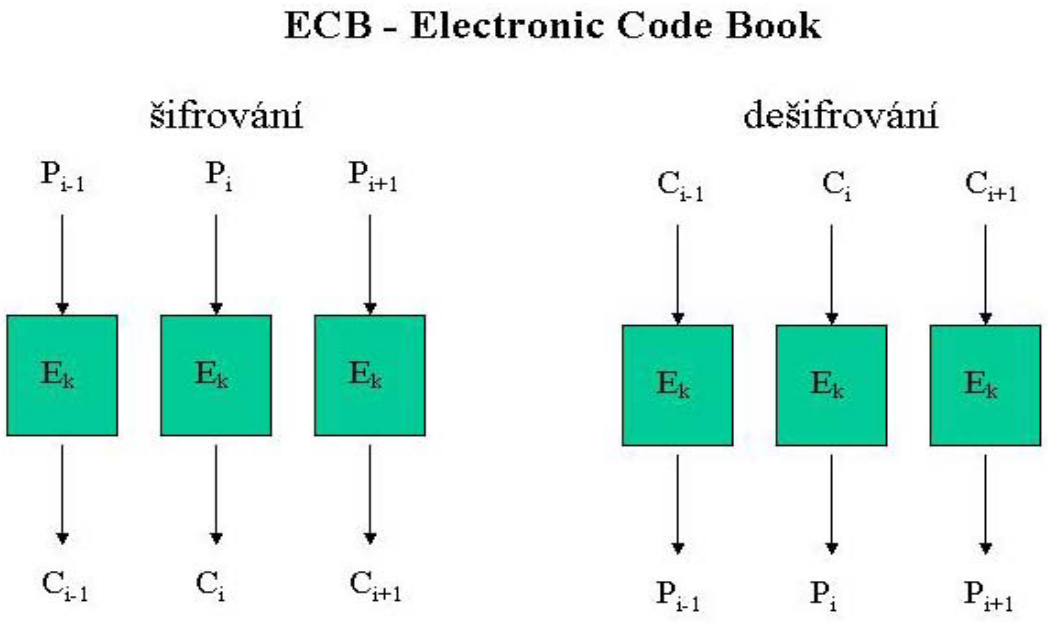
Režim činnosti je pojem, který souvisí s blokovými algoritmy šifrování (tj. s kryptografickými algoritmy, které šifrují zprávu po blocích pevné délky, např. o velikosti 64, 128 nebo 256 bitů) při šifrování delších dat (zpráv), než je velikost bloku. Režimy činnosti pro kryptografický algoritmus DES byly v USA standardizovány už v roce 1980 v publikaci FIPS PUB 81 a později v národní normě ANSI X3.106-1983. Tyto režimy činnosti jsou doporučeným způsobem, jak použít algoritmus DES pro zašifrování delšího proudu bitů. Organizace ISO tyto režimy činnosti normalizovala jako režimy činnosti libovolného blokového šifrovače a výsledkem jsou dvě normy: ISO 8372 - 1987 (režimy činnosti pro 64bitový blokový šifrovač) a ISO/IEC 10116 - 1997 (režimy činnosti pro n-bitový blokový šifrovač). Všechny zmíněné normy (FIPS, ANSI a ISO) zavádějí čtyři režimy činnosti:

- Režim *ECB* (Electronic Code Book)
- Režim *CBC* (Cipher Block Chaining)
- Režim *OFB* (Output FeedBack)
- Režim *CFB* (Ciphertext FeedBack).

V dalším textu budeme značit i-tý blok zprávy *P* (Plaintext) symbolem P_i , i-tý blok šifrového textu *C* (Ciphertext) C_i. a dále i-tý blok hesla *K* (Key) symbolem K_i . Šifrování v blokovém šifrátoru formálně splňuje vztah $C_i = E_k (P_i)$ a dešifrování $P_i = D_k (C_i)$ (kde *E* je šifrovací a *D* dešifrovací transformace).

Režim ECB

Režim ECB pracuje tak, že srozumitelný otevřený text *P* (Plaintext) je rozdělen na bloky P_i o délce odpovídající délce bloku příslušné blokové šifry a každý blok je samostatně zašifrován transformací *E* aplikací stále stejného klíče *K*. Výsledné bloky se opět spojí do jedné zprávy – šifry *C* (Ciphertext). Dešifrování se provádí opačným způsobem.



Prakticky se jedná o substituci, kdy každému bloku na vstupu odpovídá jeden blok na výstupu (v závislosti na použitém klíči). Režim činnosti ECB se v praxi používá řídce, neboť je vhodný pouze pro šifrování krátkých zpráv (např. při šifrování kryptografických klíčů nebo inicializačních parametrů), kdy nedochází k opakování částí otevřeného textu. Jinými slovy: stejné úseky otevřeného textu se při použití stejného klíče zašifrují na stejné úseky šifrového textu. Právě uvedená vlastnost dala jméno tomuto režimu činnosti - elektronická kódová kniha (Electronic Code Book). Pokud nevezmeme tuto vlastnost do úvahy, může se stát vážnou slabinou zmíněného režimu.

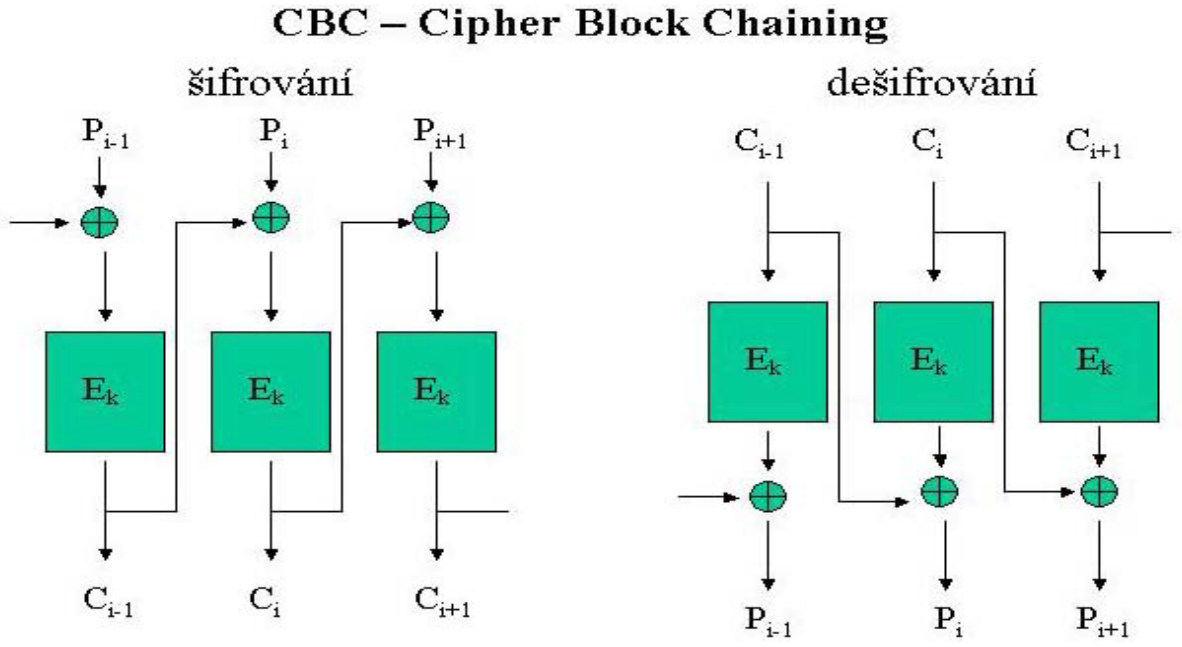
Režim CBC

Pro přenos delších zpráv, kdy je potřeba eliminovat základní nevýhodu ECB módu (stejné úseky otevřeného textu jsou zašifrované na stejné úseky šifrového textu), se používá režim činnosti CBC. Podobně jako režim ECB i režim CBC pracuje tak, že otevřený text P je rozdělen na bloky o délce odpovídající délce bloku blokového šifrovače a každý blok je blokovým šifrovačem zašifrován samostatně.

Na rozdíl od režimu ECB je však pro každý blok před jeho zašifrováním provedena operace XOR (součet mod 2) s předchozím zašifrovaným blokem. Pro první blok zprávy (který nemá žádný předchozí blok) se provádí operace XOR s tzv. *inicializačním vektorem IV*. Tím je zašifrování bloku zprávy dáno nejen bity tohoto bloku a klíčem, ale i všemi předešlými bloky zprávy. Inicializační vektor nemusí být utajován a může být přenesen v otevřené podobě např. na začátku šifrové zprávy.

Tento režim je asi nejpoužívanějším režimem pro šifrování delších zpráv. V případě, že délka šifrované zprávy není celistvým násobkem velikosti bloku, je třeba zprávu na potřebnou délku doplnit (tzv. padding). Symbolicky lze popsat činnost při tomto režimu jako $C_i = E_k (P_i \oplus C_{i-1})$.

Dešifrování lze symbolicky zapsat jako $P_i = D_k (C_i) \oplus C_{i-1}$ .Výjimkou je dešifrování prvního bloku, kdy se místo neexistujícího bloku C_0 použije inicializační vektor IV. Nevýhodou režimu CBC je skutečnost, že při vzniku chyby během přenosu bloku C_i je blok P_i zcela chybný a v bloku P_{i-1} se objeví jeden chybný bit.



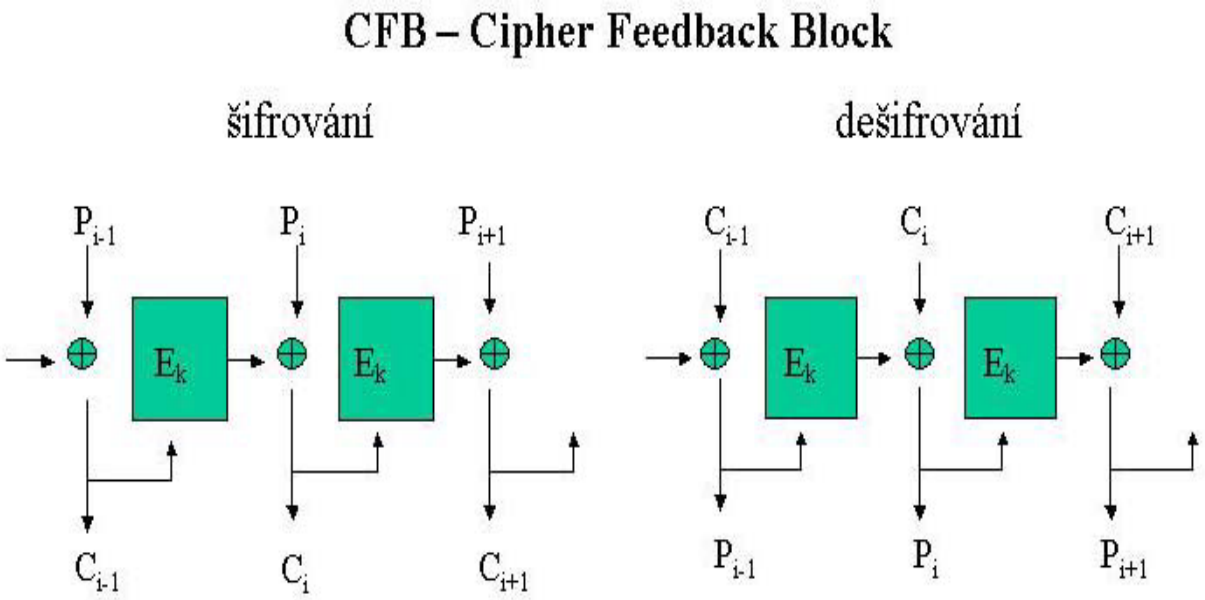
Režim CFB

U režimu CFB se na rozdíl od předchozích dvou režimů zpráva nemusí rozdělovat na bloky, odpovídající velikosti bloku blokové šifry. Místo toho je možno zprávu chápat jako plynulý proud dat o libovolné velikosti (velikost těchto dat musí být samozřejmě vyjádřena celistvým počtem bitů). V obecném případě proto musí být pro režim CFB stanoveny dva parametry *j* a *k*, kde *j* odpovídá délce úseků, na které je zpráva rozdělena, a *k* velikosti bloku blokové šifry. Z důvodu bezpečnosti musí být *j* menší nebo rovno *k* . V praxi se používá často hodnota j=8 (délka ASCII znaku) nebo mají parametry *j* a *k* stejnou hodnotu. V dalším popisu se dopustíme tohoto běžného zjednodušení, které má vliv pouze na výrazné zjednodušení formální stránky popisu tohoto režimu.

V tomto režimu se prakticky jedná o proudovou šifru. Bloková šifra zde slouží jako generátor pseudonáhodné posloupnosti (hodnota H), která je pak použita pro zašifrování otevřeného textu (zprávy) operací XOR (součet mod 2). Generátor je ovlivňován zpětnou vazbou, získanou ze zašifrovaného textu. Zpětná vazba dala tomuto režimu i název – *Ciphertext FeedBack.*

Symbolicky lze tento postup zapsat následovně. CFB je proudová šifra $C_i = P_i \oplus H_i$, $H_i = E_k (C_{i-1})$. Při šifrování prvního bloku zprávy P_1 se neexistující blok C_0 nahradí inicializačním vektorem IV. Tedy $H_1 = E_k (IV)$. Na rozdíl od CBC je nutné, aby inicializační vektor *IV* byl unikátní pro každou novou zprávu. Tj. po celou dobu používání klíče *K* musí být zajištěno, že na každou zprávu je použit jiný klíč.

Dešifrování se provádí analogicky $P_i = C_i \oplus H_i$, $H_i = E_k (C_{i-1})$.Výjimkou je dešifrování prvního bloku zprávy, kdy se místo C_0 použije inicializační vektor *IV*. Uvědomte si, že v režimu CFB se používá šifrátor pouze v režimu šifrování (označeno jako transformace *E*).



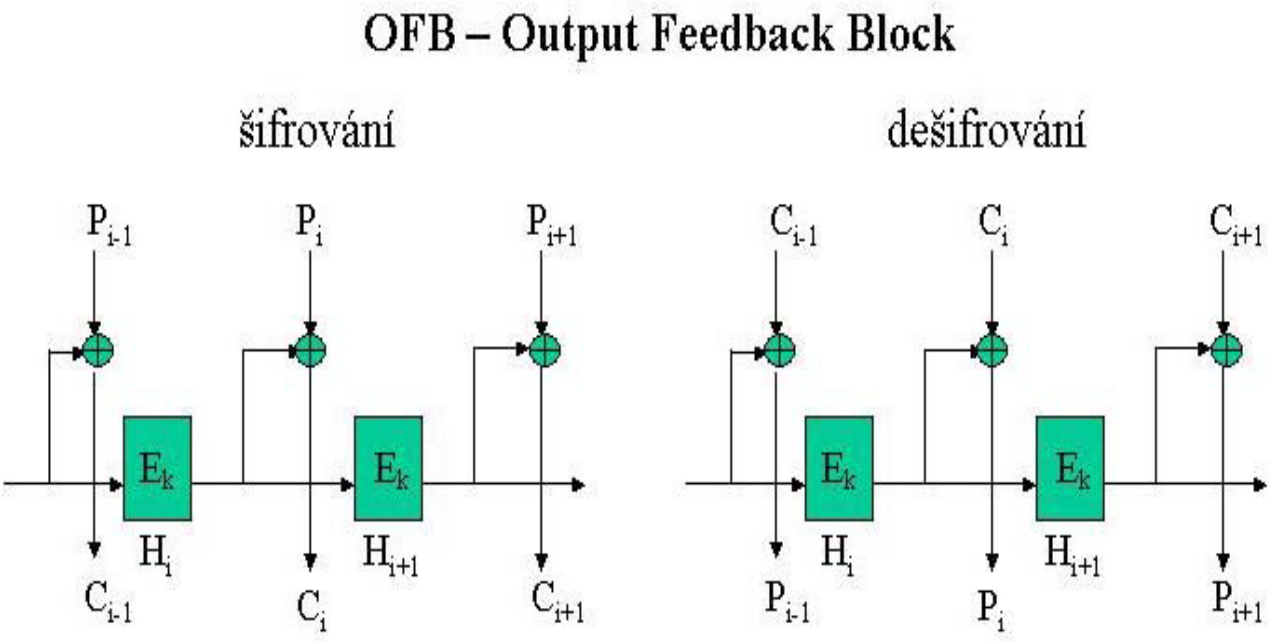
Režim OFB

U režimu OFB se obecně zpráva nerozděluje na bloky, ale opět ji lze chápat jako plynulý tok dat o libovolné velikosti. Jedná se tedy opět o proudovou šifru. Pro režim OFB je stanoven parametr *j*, který odpovídá velikosti datové struktury zprávy. Šifrovaný text se opět nestává blokovou šifrou, bloková šifra slouží jako generátor pseudonáhodné posloupnosti

(hodnota *H*), která je použita pro zašifrování otevřeného textu (zprávy) operací XOR. Generátor není ovlivňován zašifrovaným textem, ale pouze výstupem samotného generátoru. Tento typ zpětné vazby dal tomuto režimu název – *Output FeedBack*. Z hlediska bezpečnosti je nutné dodržet, aby délka zpětné vazby *j* byla stejná jako velikost šifrovaného bloku *k*.

Symbolicky lze popsat tento režim následovně. Pro jednoduchost popisu předpokládejme, že velikost parametru *j* je shodná s velikostí bloku příslušné blokové šifry. Šifrový text C_i získáme opět jako $P_i \oplus H_i$, kde heslo generuje blokový šifrátor zašifrováním předchozího bloku hesla – tj. $H_i = E_k (H_{i-1})$. Při šifrování prvního bloku zprávy P_i se neexistující blok hesla H_0 nahradí, tak jako v předchozím režimu, inicializačním vektorem *IV*. Tento inicializační vektor nemusí být utajován, ale je nutné zajistit, aby byl po dobu „života“ klíče unikátní, tedy pro každou zprávu jiný.

Dešifrováni probíhá následovně: $P_i = C_i \oplus H_i$, kde $H_i = E_k (H_{i-1})$. Výjimkou je opět dešifrování prvého bloku, kdy místo H_0 se použije inicializační vektor *IV*. V tomto režimu se používá blokový šifrátor opět pouze v režimu šifrování (transformace *E*). Výhodou režimu OFB je skutečnost, že případné chyby v přeneseném bloku šifrového textu nezpůsobí chybné dešifrování jiných bloků. Na druhé straně „ztráta“ bitu může vést ke ztrátě synchronizce přenosu. Z tohoto důvodu je nutné zajistit při přenosu nějaký jiný mechanismus, který by detekoval ztrátu synchronizace a zajistil její obnovu.



Literatura

A.Menezes, van Oorschot and Vanstone: Handbook of Applied Cryptography (CRC Press, 1997)

Schneier, B., Applied Cryptography Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, 1996

C. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 5. Prokázání vlastnictví klíče pomocí Diffie-Hellmanova algoritmu.
Jaroslav Pinkava, AEC spol. s r.o.

1. Úvod

Minulá část seriálu se zabývala vlastnostmi protokolů CRMF a CMC (Certificate Request Message Format) a také protokolem CMC. V dnešní části se budeme věnovat jinému významnému protokolu a sice protokolu, na jehož bázi majitel dvojice klíčů (soukromý a veřejný) při podání žádosti o digitální certifikát prokazuje, že je vlastníkem příslušného soukromého klíče. Toto prokazování musí být samozřejmě prováděno takovou cestou, při které nedojde k jakékoliv kompromitaci příslušného soukromého klíče.

Samotný protokol je obsažen v [1]. Jsou zde popsány dvě ověřovací metody na bázi Diffie-Hellmanovy dvojice klíčů. Tento postup je využíván např. při takových operacích jako je vytváření žádosti o certifikát dle PKCS #10. Algoritmy zde specifikované jsou přitom určeny především pro řešení situací, kdy je třeba prokázat vlastnictví klíče (tj. jejich cílem není vytváření digitálních podpisů pro obecné účely).

V [3] je definována syntaxe žádostí o certifikát. V PKCS#10 se předpokládá, že veřejný klíč, o jehož certifikát žádáme, lze použít jak pro podepisování, tak i pro šifrování. Diffie-Hellmanův algoritmus je algoritmus pro dohodu na klíči a nelze ho tedy přímo použít ani jako podepisovací ani jako šifrovací algoritmus.

Na základě DH algoritmu lze však vytvářet sdílené tajemství a toto je posléze využito pro ověření integrity. V prvním ze dvou popsaných algoritmů je konstruována tato hodnota pro určitého konkrétního ověřovatele použitím jeho veřejného klíče. Ve druhém algoritmu je tato hodnota konstruována tak, aby ji mohl využít libovolný ověřovatel.

DH-certifikátem (Difie-Hellmanovým certifikátem) budeme rozumět certifikát, jehož SubjectPublicKey je veřejnou DH hodnotou a který je podepsán libovolným podpisovým algoritmem (RSA, DSA atd.).

2. Statické DH prokázání vlastnictví klíče (DH POP)

Vlastní algoritmus probíhá následovně.

Krok 1.: Entita E zvolí parametry pro DH dohodu na výměně klíčů, což je prováděno na základě hodnot z certifikátu zamýšleného příjemce procesu POP. Přepokládejme, že jsou to DH parametry g a p (soukromým klíčem příjemce je x).

Krok 2.: Entita si vygeneruje svoji DH dvojici klíčů y (soukromý klíč) a g^y mod p (veřejný klíč).

Krok 3.: Samotné POP probíhá následovně:

a) je spočtena hodnota, která bude podepisována (pro objekt dle rfc2314 je to DER kódované pole certificationRequestInfo reprezentované jako oktetový řetězec). Na získaný "text" použijeme HMAC-SHA-1.

b) Obě strany spočtou sdílenou utajovanou DH hodnotu: $ZZ = g^{xy} \bmod p$.

c) Je spočten dočasný klíč K jako

K = SHA1(LeadingInfo | ZZ | TrailingInfo), kde "|" je konkatenace.

LeadingInfo ::= Subject Distinguished Name z certifikátu
TrailingInfo ::= Issuer Distinguished Name z certifikátu

d) Je spočten HMAC-SHA1 pro data "text" dle rfc2104 následovně:

SHA1(K XOR opad, SHA1(K XOR ipad, text))

kde, opad (outer pad) = byte 0x36 opakovaný 64 krát a
ipad (inner pad) = byte 0x5C opakovaný 64 krát.
(podrobněji v [1] či v [4]).

e) Výstup z bodu d) je vyjádřena v podobě bitového řetězce (= hodnota podpisu).
Ověřovací strana provede kroky a) až d) a pak porovná získaný výsledek se zaslanou hodnotou.

Pokud obě hodnoty souhlasí, vyplývá z toho následující:

a1) Entita E je vlastníkem příslušného soukromého klíče, který odpovídá veřejnému klíči obsaženému v žádosti o certifikát (potřebovala soukromý klíč k výpočtu sdíleného tajemství).
b1) Pouze ten adresát, kterému poslala entita žádost může tuto žádost ověřit (k výpočtu sdíleného tajemství je třeba jeho soukromý klíč). Tato skutečnost např. chrání CA před "zlodějskými" certifikačními autoritami.

3. Podpis na bázi diskrétního logaritmu

Pokud budeme pro celou PKI používat jedinou množinu parametrů, pak lze konstruovat útoky směřující současně na všechny klíče. Z tohoto důvodu je vytvářen POP pro DH klíče, který nepoužívá obecnou množinu parametrů.

V následujícím popisu algoritmu nejsou sice splněny požadavky normy FIPS-186, ale pokud je použita metoda generování klíčů z normy ANSI X9.42, budou splněny i tyto požadavky. Dodatečným požadavkem je existence parametru q (jeho existence umožňuje ochranu před útokem malé podgrupy).

Značení:
p je velké prvočíslo
$g = h^{(p-1)/q} \bmod p$,
kde h je přirozené číslo, $1 < h < p-1$, a $h^{(p-1)} \bmod q > 1$ (g je řádu q mod p)

q je velké prvočíslo
j je velké přirozené číslo, pro které $p = qj + 1$
x je náhodně či pseudonáhodně vygenerované přirozené číslo, $1 < x < q$
y = g^x mod p

Norma FIPS-186 zavádí rovněž určitá omezení na velikosti parametrů. Délka q musí být 160 bitů a délka p musí být 1024 bitů. Tyto požadavky nejsou v dokumentu formulovány, pouze délka q musí být minimálně 160 bitů. Musí být potom použita taková metoda vytváření otisku zprávy, která umožňuje expandovat délku hashe na potřebnou délku.

Následující algoritmus generuje hodnotu m, která je následně podepisována.

Nechť L je velikost q (tj. $2^L \leq q < 2^{L+1}$). Nechť M je zpráva, kterou podepisujeme.

1. Spočteme d = SHA-1(M).

2. Pokud L == 160 pak m = d.

3. Pokud L > 160 pak:

a) Nechť n = ⌈L / 160⌉, (celá část po dělení)
b) Položíme m = d,
c) pro i = 0 to n - 1 m = m | SHA(m), kde "|" značí konkatenaci.
d) m = LEFTMOST(m, L-1), kde výsledkem operace LEFTMOST je levých L-1 bitů m.

Pro výsledek platí $0 \leq m < q$.

Výsledkem podpisového algoritmu je dvojice čísel (r,s) tvořící podpis:

1. Generujeme náhodné či pseudonáhodné k, tak, že $0 < k^{-1} < q$.
2. Spočteme $r = (g^k \bmod p) \bmod q$.
3. Je-li r rovno nule, vracíme se ke kroku 1.
4. Spočteme $s = k^{-m - xr} \bmod q$.
5. Je-li s rovno nule, vracíme se ke kroku 1.

Verifikace podpisu je složitější než pro obvyklé DSA, neboť některé předpoklady o hodnotách parametrů zde apriori neplatí.

Máme k dispozici ověřovanou zprávu m, hodnoty (r,s) a klíčové parametry.
Ověříme zda p a q jsou prvočísla.
Ověříme, že q je faktor p-1, pokud některé z těchto prvních dvou ověření neplatí, pak podpis nemůže být verifikován.

Dále:
3. Ověříme, že r a s jsou v intervalu [1, q-1].
4. Spočteme $w = (s^{-1}) \bmod q$.
5. Spočteme u1 = m*w mod q.
6. Spočteme u2 = r*w mod q.
7. Spočteme $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$.
8. Spočteme v a r, jsou-li shodné s ověřovanými hodnotami, pak podpis je verifikován.

4. Některé poznámky

Ve statickém DH POP algoritmu může příslušnou hodnotu generovat kterákoliv strana. Tento algoritmus proto může sloužit pouze pro ověření integrity, nikoliv pro prokazování původu. Podpis na bázi diskrétního logaritmu umožňuje obojí, tj. i ověření integrity i ověření původu.

Celá bezpečnost popsaného systému spočívá v utajení příslušných soukromých klíčů. Kompromitace soukromých klíčů vede ke kompromitaci všech příslušných zpráv, které se opírají o použití těchto klíčů. Velikou pozornost je třeba věnovat volbě parametrů.

Ještě k přílohám materiálu [1] :

Příloha A obsahuje modul ASN.1 .

Příloha B obsahuje příklad statického DH důkazu vlastnictví klíče (dle výše uvedeného popisu v odstavci 2). Verifikace (ověření) vyžaduje mít k dispozici veřejný klíč CA, certifikát CA a vygenerovanou žádost o dertifikát.

Příloha C. obsahuje příklad podpisu na bázi diskrétního logaritmu.
Nejprve je generován DH klíč (parametr q má délku 256 bitů). Následně je vytvořena hodnota, která bude podepisována a je hashována pomocí SHA-1. Takto získaný hash je rozšířen (dalším použitím SHA-1 na výsledek původního hashe) na celkem 255 bitů. a konečně je spočten podpis této hodnoty.

5. Literatura

[1] Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875),
(http://www.ietf.cnri.reston.va.us/rfc/rfc2875.txt)

[2] Federal Information Processing Standards Publication (FIPS PUB) 186, "Digital Signature Standard", 1994 May

[3] Kaliski, B., "PKCS #10: Certification Request Syntax v1.5", RFC 2314, October 1997.

[4] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February1997

[5] Housley, R., Ford, W., Polk, W., and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January 1999

[6] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.

D. Elektronický podpis - projekty v Evropské Unii. Část I.

Jaroslav Pinkava, AEC spol. s r.o.

V rámci prací EU nad dokumenty v oblasti elekronického podpisu (pracovní skupina CEN/ISSS) proběhly v loňském létě (červen - září) práce na projektu "A pre-inventory of smart card based PKI projects within the EU" (http://www.cenorm.be/isss/Projects/SCC-TB2/default.htm).

Získané výsledky byly zpracovány v materiálu:
Mitrakas, Andreas; Blivet, Laurent; Moyal, Moise: A pre-inventory of smart card based PKI projects within the EU, version 1.3., February 2002
a čtenářům zde předkládáme jeho podstatný výtah.

Samotný materiál je velmi zajímavý a umožňuje získat poměrně komplexní pohled na problematiku projektů spojených s využíváním **čipových karet** v dnešní Evropě.

Pravda je, že tento typ materiálů poměrně rychle zastarává, od loňského září se objevila (např. v Německu a Španělsku) celá řada novějších aktivit. Na druhou stranu stále jeho přínosem je určité shrnutí existujících zkušeností v dané oblasti.

1. Úvod

Evropská komise přijala strategickou iniciativu eEurope, jejímž úkolem je akcelerovat přechod evropských ekonomik do digitální éry. Důležitou částí této iniciativy je eEurope Smart Card Charter (eE SCC), která má zase za úkol stimulovat akceptaci a využití čipových karet v celé Evropě. Plány zahrnují jak uspokojení potřeb jednotlivých občanů, tak i podnikatelské sféry. Týká se to podnikatelských záměrů, multifunkcionality a interoperability systémů a infrastruktury ve smyslu zabezpečení důvěryhodnosti všech aspektů v dodávkách služeb.

Zpráva, která je zde citována, dává předběžný pohled na projekty PKI, které se opírají o využití čipových karet. Předběžnost je zde chápána v tom smyslu, že zpráva zatím neobsahuje hlubší analýzu problematiky. Materiál je součástí dokumentů (jako draft) v aktivitách eEurope, konkrétně v eE SCC, Trailblazer 2 on Identification and Authentication (TB2). Cílem TB2 je vytvořit kdo konce roku 2002 společnou , funkční a přijatelnou platformu pro všechny elektronické transakce ve smyslu využití identifikace, autentizace a digitálních podpisů. Práce TB2 se tedy opírá o PKI a čipové karty.

PKI (Public Key Infrastructure) je považována za vhodnou technologii pro implementaci požadavků Směrnice EU 99/93 pro elektronické podpisy a stejně tak pro splnění požadavků uživatelů otevřených sítí. Probíhá široká práce na vytváření norem v oblasti elektronického podpisu.

Čipové karty jsou považovány za spolehlivé medium pro zabezpečení přístupu k široké řadě služeb, které se přitom opírají o širokou škálu technologických platforem. Elektronický obchod či mobilní obchodní aplikace jsou příklady takových platforem.

Význam samotných problematik jako PKI a technologií čipových karet v posledních letech zcela nepochybně roste. Vzájemná kombinace těchto dvou bazických technologií je považována za vhodný prostředek pro splnění požadavků na identifikaci a autentizaci v rámci širokých sfér aplikací. Průmysl a standardizační orgány hrají důležitou roli při vytváření celé řady standardizačních iniciativ včetně European Electronic Signature Standardisation Initiative (EESSI). Je konstatováno, že v současné době existuje pouze malý počet reálně žijících projektů, které obě tyto technologie (PKI a karty) smysluplně kombinují.

V současnosti běží více takovýchto projektů v iniciativách veřejného sektoru a sociálního zabezpečení. V soukromé sféře začaly již dříve banky s implementacemi PKI, které se opíralo o využívání čipových karet. Rozsáhlou cílovou agendou v dané oblasti jsou identifikační karty sloužící jako průkaz totožnosti jednotlivých občanů. Čipové karty jsou důležitým nástrojem pro zjišťování elektronické identity v on-line službách. Slouží zde jakožto bezpečnostní prvek pro zjišťování totožnosti osob a to jak ve sféře veřejné tak i soukromé.

V zemích, kde byly nastartovány elektronické identifikační karty (Švédsko, Finsko) je vývoj projektů založených na PKI a čipových kartách snazší, než v ostatních členských zemích. Část jako doplňková služba identifikační karty je využíváno celé řady dalších služeb, které jsou přitom podporovány toutéž kartou (např. zdravotnictví, volební právo, sociální zabezpečení atd.). Obdobným způsobem funguje i celá řada lokálních služeb (v závislosti na místních požadavcích a potřebách) – doprava, vzdělávání atd.

Vlastní přehled uvedený v materiálu vznikal v červenci a srpnu 2001. Za tímto účelem byl vytvořen dotazník, který byl zaslán manažerům jednotlivých projektů. Souběžně byly využity některé veřejné zdroje. Materiál nebyl vytvářen s cílem hodnotit kvalitu jednotlivých projektů.

Vzhledem k tomu, že se jedná o předběžnou analýzu, byl identifikován pouze omezený počet projektů, které mohou být dále hlouběji analyzovány. Za tímto účelem byla použita následující kriteria:
- zralost projektu (plány, které budou implementovány, probíhající piloty, fáze ve které se projekt nachází). Přednost mají samozřejmě projekty v rozvinutých fázích, tam kde jsou již využívány čipové karty obsahující digitální certifikáty
- velikost projektu (např. počet karet, certifikátů atd.). Velké projekty obvykle používají hlubší technické analýzy a jsou obecně složitější z organizačního hlediska
do úvahy byla brána i geografická a odvětvová kriteria s cílem vytvořit rovnovážný přístup ve vztahu k ověřovaným projektům ve smyslu jejich zaměření a dosahu
- přístup k manažeru projektu, spolehlivost zdrojů a ochota sdílet informace projektového týmu.

Jedním z důležitých aspektů přehledu byla snaha ozřejmit vliv materiálů EESSI (viz např. problematika evropských norem v oblasti elektronického podpisu, materiály ETSI a CEN/ISSS – články J. Pinkavy v Crypto-Worldu) a směrnice EU pro elektronický podpis.

2. Vybrané projekty

Následuje seznam analyzovaných projektů:

Jméno projektu	Popis	Kategorie	Statut	Země
ABN Amro-Identrus	B2B autentizace, digitální podpis, platební a obch. styk	soukromý sektor	Plně rozvinuto	globální
AdeP	víceužitková občanská karta	identifikační karta	projektové stadium	Francie
Finish Citizen Identity card	elektronická občanská identifikační karta	identifikační karta	rozvinuto	Finsko
French Notaries	Autentizace a digitální podpisy pro výměnu dokumentů mezi notáři	Iniciativa profesní asociace	rozvinuto	Francie
GIP-CPS	Autentizace a digitální podpisy ve zdravotnictví	Zdravotní a sociální zabezpečení	rozvinuto	Francie
Italian Citizen Identity card	elektronická občanská identifikační karta	identifikační karta	Pilotní projekt	Itálie
PKI Overheid	Víceúčelové identifikační řešení	Víceúčelové	projektové stadium	Holandsko
Posten AB	Víceúčelová občanská identifikační karta	identifikační karta	rozvinuto	Švédsko
Satakunta	Aplikace pro sociální zabezpečení na bázi Finské identifikační karty	Zdravotní a sociální zabezpečení	Pilotní projekt	Finsko
Social security and Communidad Valenciana public services	Ověření totožnosti	Zdravotní a sociální zabezpečení	projektové stadium	Španělsko
TEKES	Aplikace pro sociální zabezpečení na bázi Finské identifikační karty	Zdravotní a sociální zabezpečení	rozvinuto	Finsko

Analyzované projekty jsou převážně koncentrovány na vládní aplikace nebo jsou vedeny velkými soukromými iniciativami. Všechny jsou směrovány pro využití v rámci velkých populací (miliony uživatelů).

Omezujícím faktorem u takovýchto projektů bývá často jejich cena. Přístupy k financování bývají různého typu:
- plně veřejně financované projekty (většinou obecného charakteru, jako nucené a národní identifikační karty)
- karty a certifikáty, které jsou prodávány koncovým uživatelům, obvykle jsou svázány s aplikací.

3. Analýza vybraných projektů

V analýze jsou brány do úvahy organizační, technické a legislativní aspekty.

A. Investiční a organizační aspekty:

Pokud chceme získat celkový přehled projektu z hlediska daných aspektů, je třeba popsat:
investiční model: cena na jednoho uživatele, návratnost investic;
- postup projektu: současný stav, plán, velikost projektu;
- zjištěné význačné problémy: technické, politické, legislativní;
- procesy: registrace, certifikace, personalizace.

Zvažované projekty se nachází v různých vývojových stadiích, používají různé investiční modely (založené však většinou na využití čipových karet v rámci implementací PKI). Rozdíly vznikají jak díky rozličným fázím, ve kterých se projekty nachází, tak i díky různým obchodním cílům jednotlivých projektů.

V rámci projektu **ABN AMRO – Identrus** (zahájen v roce 1999) se spojilo více než 50 finančních institucí na využívání jednoho bankovního akreditačního schématu. Tyto instituce dnes reprezentují více než 133 zemí a miliony obchodních vazeb. Základní investiční model projektu zahrnuje platby dle typu transakcí a opírá seve své bázi o zákazníky typu korporací. Model umožňuje elektronický podpis na čipových kartách a ověřování podpisu pro jednotlivé aplikace.

Multifunkcionální projekt **AdeP identity Card** (vydáno zatím 500 čipových karet) se nachází v současnosti (léto 2001) ve fázi testování prototypu. Další podstatné rozšíření prací je plánováno na konec roku 2001 a začátek roku 2002. Má se přitom již týkat jednotlivých francouzských občanů, korporací, veřejné správy a místních úřadů. Předpokládá se, že v roce 2005 bude zahrnovat 3000 čipových karet. Projekt se stal ve Francii referenčním, ve smyslu aplikací zákona o elektronickém podpisu (vzhledem k certifikovaným prostředkům). Použitý investiční model vychází z plateb za každou činnost, která je ověřována a zabezpečována pomocí čipových karet. Projekt v tomto počátečním stadiu je financován vládními zdroji.

Ve Finsku v rámci projektu **Citizen identity card (F)** bylo již vydáno zhruba 9500 karet. Cílem je poskytnout tyto karty celé finské populaci. Projekt nedosáhl svých cílů a počet vydaných karet zůstává nízkým. Projekt vychází z investičního modelu, kde kartu může získat každý občan, který si ji vyžádá. Je to však dobrovolné. Každá karta je perzonalizována a

obsahuje dva certifikáty. Přístup k adresářům a odvolávání certifikátů je bezplatné. Je publikován seznam doporučených čteček karet. Samotná karta s certifikáty stojí asi 27 Euro, celý paket obsahující i software a čtečku stojí zhruba 100 Euro. Dalšímu rozvoji projektu stojí v cestě některé legislativní nedostatky a nepřítomnost příslušných elektronických služeb.

Projekt **French Notaries** byl zahájen v roce 1999. Cílovými objekty jsou notářství a jejich zaměstnanci. V současné době bylo vydáno cca 3500 karet a paketů pro elektronický podpis. Výhledově se přepokládá, že v systému bude vydáno 22000 karet. Technických cílů v rámci projektu bylo dosaženo, ale počet transakcí stále zůstává nízký. Cena jednoho paketu je asi 150 Euro (obsahuje čtečku a software). Karty a certifikáty jsou bezplatné.

Projekt **GIP-CPS** ve Francii se nachází již ve stadiu vlastního využívání (zatím 350 karet). Během dalších tří až pěti let se předpokládá, že bude zahrnovat až jeden milion karet. Cena za používání karty a návazných služeb je menší než 30 Euro. Sama karta je bezplatná. Dlouhodobě se předpokládá takto vytvoření bezpečného IT systému ve zdravotnictví. Projekt měl určité problémy s podpůrnými organizacemi z veřejné správy (je jich více než 20) a také existují určité problémy s přípravou zdravotního personálu.

Italský projekt **Citizen identity card (I)** byl zahájen v roce 2001, v rámci pilotního projektu bylo vydáno sto tisíc karet. Dle předpokladů bude v roce 2005 vydáno osm milionů karet. V projektu existují určité skluzy, které vznikly díky technickým problémům.

Nizozemský projekt **PKI Overheid** je multifunkcionální řešení. V současné době je ve stadiu veřejného projednávání příslušných požadavků, běží několik pilotních projektů. Vlastní rozvoj pro široké aplikace je předpokládán v letech 2003 až 2005 (až 20 milionů karet). Investiční model je však ještě nutné dopracovat (i z hlediska nákladů na jednotlivého uživatele).

Ve Švédsku **Posten Ab identity card** project již vydal 50 000 karet. Cílovou populací je veškeré švédské obyvatelstvo. projekt byl zahájen již roce 1996. Paket obsahující kartu a čtečku stojí od 53 do 63 Euro. Certifikáty platí dva roky a stojí od 33 do 42 Euro. Využívání adresářů a odvolávání certifikátů je bezplatné. Problémem je, že některé aplikace zatím neobsahují PKI interface a k tomu navazující software.

Finský **Satakunta project** je orientován na 10 000 profesionálů a 1000 občanů (jako pilotní projekt). Existují zde některé technické problémy spojené s updatem osobních údajů na kartách a otázkami autentizace a autorizace. Existuje pevný poplatek za kartu (50 Euro) shodný jak pro profesionály tak i občany.

Ve Španělsku je připravován projekt **Social security and Communidad Valenciana**. V červnu 2002 má být zahájen pilotní projekt. Plné využití předpokládá 5 miliónů karet (v roce 2003). Cean karty je 12 Euro (občané platí z toho polovinu).

Finský sociální projekt **TEKES** zpřístupnil svou první funkční softwarovou verzi v létě 2001. Karty vydává vládní agentura Population Register Centre. Jsou předpokládány roční poplatky. Systém bude využívat identifikační karty vydávané Finnish Population Register.

Všechny investiční modely popsané ve výše vybraných projektech se potýkaly s určitými problémy. Většina projektů plánuje dlouhodobou návratnost investic. Oblastmi ve kterých je možné počítat s určitými vylepšeními jsou:
- rostoucí počet transakcí na jednoho uživatele;
- rostoucí počet aplikací využívajících PKI jako bezpečnostní vrstvu.

B. Technické aspekty

Z hlediska technických aspektů zkoumaných projektů (kombinace PKI a čipových karet) existují určité momenty, jejichž pečlivé zvážení může vést k zvýšení efektivnosti realizovaných projektů:
- požadavky na shodu s existujícími normami s cílem zabezpečit interoperabilitu různých řešení i aplikací připravovaných do budoucna;
- je požadována otevřenost řešeni, vzhledem k tomu, že na přípravě a fungování většiny projektů se musí podílet více stran, předpokládá se také zapojení dalších stran v budoucnu;
- předpokládán je posun směrem k digitálnímu podpisu s veškerými legislativními důsledky; do budoucna budou využívány kvalitnější technologie.

Stejně tak je i používání čipových karet spojeno s určitými podmínkami, které je nutno zvažovat pro jejich konkrétní výběr:
- je požadována důsledná ochrana soukromého klíče;
- je požadováno řešení, které je vstřícné a pohodlné pro samotného uživatele;
- nezbytné zvážit vliv národní legislativy a existujících regulačních opatření ve vztahu ke konkrétnímu připravovanému řešení (a to jak z hlediska současných tak i budoucích požadavků);
- kontinuita ve vztahu k současným infrastrukturám využívajícím čipové karty.

Shoda s existujícími bezpečnostními normami (FIPS, ISO 15408 - Common Criteria,…) je považována za klíčový moment pro zajištění kompatibility s legislativními požadavky ve vztahu k digitálním podpisům. Zatím existuje jen omezený počet testovaných a akreditovaných čipových karet.

Ve většině projektů splývá doba platnosti certifikátů s dobou platnosti čipových karet. K často využívaným normám (v analyzovaných projektech) patří: X.509 v3, CRLv2, OCSP, PKCS11 a Crypto API CSP, PKCS #15 a PC/SC.

C. Legislativní aspekty

Všechny projekty deklarují shodu se záměry Směrnice EU 99/93 o elektronickém podpisu. Většina projektů si klade za cíl vydávání kvalifikovaných certifikátů a akreditaci příslušné certifikační autority.

(v příštím čísle Crypto-Worldu 9/2002 bude uvedeno dokončení tohoto článku)

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

Jan Hobza, ÚOOÚ Praha

Tento článek se zabývá především analýzou slovenského zákona se zaměřením na odlišnosti v české a slovenské úpravě elektronického podpisu. Cílem je poukázat na rozdíly v přístupu obou předpisů k dané problematice a upozornit na možné důsledky těchto odlišností. Úmyslem autora v žádném případě není kritizovat ten či onen právní předpis ale pokusit se o objektivní zhodnocení.

V březnu tohoto roku přijala slovenská Národní rada zákon č. 215/2002 Z. z. o elektronickom podpise [1]. Prvotním motivem pro přijetí zákona byla především snaha zavést do slovenského právního řádu institut elektronického podpisu a následovat tak trend evropských států. Důvodová zpráva k zákonu dále deklaruje snahu o harmonizaci právního řádu s požadavky Směrnice 1999/93/ES o elektronických podpisech [2]. Bylo tedy možné předpokládat, že slovenský zákon bude velmi podobný svým evropským předchůdcům. Realita je však poněkud jiná a některá ustanovení slovenského zákona jsou dosti odlišná i od českého zákona o elektronickém podpisu [3].

Subjektivní působnost slovenského zákona o elektronickém podpisu je upravena v § 1. Zatímco český zákon upravuje především práva a povinnosti subjektů při vydávání, používání a správě kvalifikovaných certifikátů (tedy akreditovaných poskytovatelů, poskytovatelů podle § 6 českého zákona a podepisující a spoléhající se strany, když odhlédneme od pravomocí Úřadu), slovenský zákon vymezuje svou subjektivní působnost negativně. Tj. upravuje práva a povinnosti při vydávání všech certifikátů pro elektronické podpisy, kromě certifikačních služeb v uzavřených systémech a kromě používání elektronického podpisu v rámci zákona o utajovaných skutečnostech. Důsledkem toho je, že veškeré certifikační autority (tedy i neakreditované), které vydávají na Slovensku certifikáty v otevřených systémech, musí splňovat podmínky slovenského zákona o elektronickém podpisu. Poskytování certifikačních služeb je podnikatelskou činností ve smyslu obchodního zákoníku. Kromě z toho vyplývajících povinností musí tedy certifikační autorita splnit ještě další povinnosti stanovené tímto zákonem, kterými jsou mimo jiné i podrobení se kontrole Úřadu (Národný bezpečnostný úrad), vypracování bezpečnostních pravidel pro výkon certifikačních činností, archivace dokumentace a další. Zákon nestanoví, že výše uvedené postupy a povinnosti (pro neakreditované certifikační autority) by měl konkretizovat prováděcí předpis. Zda tedy bude pro běžné certifikační autority splnění těchto nových povinností pouze formální záležitostí, či zda se bude jednat o zásadní zásah do fungování podniku, bude záležet především na jejich výchozích podmínkách a schopnostech. V každém případě jejich nesplnění může mít za následek i ukončení činnosti či vysoké pokuty udělené Úřadem.

Výše uvedený přístup bude mít jistě pozitivní vliv na míru důvěryhodnosti veškerých slovenských certifikačních autorit. Motivací pro takovou zákonnou úpravu zřejmě mohl být článek 5.2 Směrnice, který ukládá členským státům nediskriminovat v soudní praxi elektronické podpisy pouze z důvodu, že se jedná o nekvalifikované certifikáty, nezaručené podpisy či z důvodu jejich elektronické formy. Směrnice však již neupravuje náležitosti těchto nekvalifikovaných služeb a po členských státech již nevyžaduje, aby i tyto služby omezily technickými regulacemi. Negativním důsledkem takového opatření může být i odchod některých poskytovatelů ze slovenského trhu pro nemožnost splnění zákonných podmínek. V každém případě je takto nastavená úroveň bezpečnosti ojedinělá a pravděpodobně jde ještě nad rámec Směrnice 1999/93/ES.

V nově vznikajících dokumentech skupin CEN/ISSS a ETSI ESI je zřejmá snaha upravit i zmíněnou oblast nekvalifikovaných certifikátů (Např. [4, 5]). Přístup je ovšem z jiného úhlu, než který zvolil slovenský zákonodárce. Úprava tzv. nekvalifikované oblasti se týká akreditovaných poskytovatelů certifikačních služeb, kteří již vydávají kvalifikované certifikáty a zároveň vydávají i nekvalifikované certifikáty. Účelem je bezpečné oddělení obou služeb, které se ve svém fyzickém i režimovém zabezpečení mohou lišit a je tedy třeba zajistit bezpečnost postupů při vydávání kvalifikovaných certifikátů ve vztahu k prostředí. Jelikož se tyto dokumenty (technické specifikace, technické regulace apod.) vztahují pouze na oblast definovanou v příloze II Směrnice, nedají se jednoduše aplikovat na všechny poskytovatele certifikačních služeb.

Slovenský zákon definuje v § 4 pojem zaručený elektronický podpis. Jedná se o elektronický podpis (tedy je vytvořený soukromým klíčem a veřejným klíčem se dá ověřit integrita zprávy), který je možné vytvořit pouze pomocí bezpečného zařízení pro vytváření podpisu, způsob jeho vytvoření umožňuje určit podepisující osobu a je založený na kvalifikovaném certifikátu. Kvalifikované certifikáty je oprávněn vydávat pouze akreditovaný poskytovatel a bezpečné zařízení musí splňovat podmínky prováděcího předpisu, který vydá NBÚ. Zákon definuje i platnost zaručeného elektronického podpisu. Ten je platný, pokud existuje kvalifikovaný certifikáty pro daný soukromý klíč, dále pokud je prokazatelné, že tento certifikát byl platný v době podpisu a dále pokud podepisovaná zpráva nebyla změněna. NBÚ stanoví způsob vytváření (algoritmy a parametry) zaručeného elektronického podpisu ve zvláštním prováděcím předpisu.

Výše uvedené vlastnosti popisují v dokumentech ETSI ESI tzv. kvalifikovaný elektronický podpis [4, 6], tj. podpis podle článku 5.1 Směrnice. Pro takový elektronický podpis mají členské státy vytvořit právní podmínky, aby měl stejné účinky vůči elektronickým podepisovaným datům, jako má vlastnoruční podpis ve vztahu k textu na papíře. Nejedná se ovšem o požadavek na „zrovnoprávnění“ vlastnoručních a elektronických podpisů, jak se často mylně prezentuje (o tom více v příštím dílu).

Český zákon o elektronickém podpisu definuje zaručený elektronický podpis stejně jako Směrnice ES. Tedy nezávisle na certifikátu, nezávisle na prostředku pro vytváření a jeho platnost výslovně neodvozuje od prokazatelnosti času jeho vytvoření.

Rozdílnost českého a slovenského přístupu k zaručenému elektronickému podpisu má na každé straně řadu výhod a řadu nevýhod a pouze podtrhuje odlišnost v přístupu k danému problému. Český zákon nevyžaduje použití bezpečných prostředků pro vytváření podpisu v žádné situaci. Vzhledem k výši nákladů na pořízení takového prostředku se umožňuje poměrně široké skupině uživatelů používat elektronický podpis podle zákona o elektronickém podpisu. Na druhé straně zde chybí kompatibilita se článkem 5.1 Směrnice. Slovenský zaručený podpis pak může být velmi náročný na finanční prostředky uživatelů. To bude záviset na úrovni bezpečnosti bezpečných zařízení pro elektronické podpisy, kterou nastaví NBÚ svými předpisy. Pokud se však bude snažit držet krok s EU, pak tato úroveň bude odpovídat EAL 4 či EAL 4+. Dále bude záležet na konkretizaci požadavku na určení času vytvoření podpisu. Pokud se za prokazatelné bude považovat pouze časové razítko k podepsanému dokumentu, pak zde může vzniknout i technologický problém pro poskytovatele certifikačních služeb.

Slovenský zákon je v plnění požadavku článku 5.1 Směrnice velmi důsledný. Naopak svou definicí běžného elektronického podpisu, která nezmiňuje autentizaci podepisující osoby (tedy hlavní požadavek Směrnice 1999/93/ES na elektronické podpisy), opomíjí požadavky článku 5.2 Směrnice ES. Můžeme samozřejmě předpokládat, že při volném hodnocení důkazů soud přihlédne i běžnému elektronickému podpisu daného dokumentu, ovšem pouze za účelem ověření jeho integrity, nikoli autenticity podepisující osoby. K tomu přispívají i

provedené novely hlavních právních předpisů a především novela občanského zákoníku. K tomuto tématu se vrátíme v příštím dílu.

[1] Zákon č. 215/2002 Z.z.,o elektronickom podpise a o zmene a doplnení niektorých zákonov http://www.zbierka.sk/zz02/02-z215.pdf
[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures http://www.volny.cz/honzahobza/Directive.pdf
[3] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ve znění zákona č. 226/2002 Sb. http://www.volny.cz/honzahobza/227-2000.htm
[4] Policy requirement for certification authorities issuing qualified certificates TS 101 456
[5] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
[6] Final Report of the EESSI Expert Team 20th July 1999

F. Malá poznámka k právnímu významu pojmu listina se zřetelem k jeho podepisování[1]

JUDr. Ján Matejka, Ústav státu a práva AV ČR

I. Místo úvodu

Jsme svědky dosud nejrozsáhlejšího rozkvětu informačních technologií v historii naší společnosti. Užívání mobilních telefonů, počítačů a Internetu a řady dalších elektronických prvků se stalo během několika posledních let prakticky běžnou součástí našeho života. Dosud standardní (tradiční) pojetí se tak postupně nahrazují jinými, resp. novými či stále novějšími koncepcemi a hledisky. Mezi jedno z takovýchto „nových" pojetí, kterého jsme v současné době přímými svědky, patří také přístup k pojmu „listina", resp. „písemnost" a chcete-li, také pojmu „podpis".
Mým přáním je podat systematický výklad alespoň těch nejdůležitějších otázek souvisejících s právním významem pojmu „listina", resp. písemnost a to z pohledu soukromého práva a se zřetelem k podepisování.

II. Podpis alias náležitost některých písemných právních úkonů

Samotný právní význam podpisu vyplývá především ze skutečnosti, že **podpis jednající osoby je předpokladem platnosti písemných právních úkonů** (§ 40 odst. 3 občanského zákoníku[2]). V tomto smyslu tedy podpis navenek osvědčuje určitý akt, v našem případě tedy právní úkon (např. uzavření smlouvy).

Písemná forma právního jednání tak tedy kromě jiných obecných náležitostí[3] vyžaduje, aby byl příslušný projev vůle zachycen na médiu, které má právní povahu listiny a dále pak aby byl tento projev vůle podepsán. O tom, co je listina v právním smyslu neobsahuje – až na jednu výjimku – náš právní řád jedinou výslovnou zmínku. Řada zákonných ustanovení však o listině poměrně často hovoří. **Legální definice listiny ale chybí**.[4]

Nezbývá než souhlasit s K. Eliášem[5], že **nejde o vytýkatelný nedostatek současné právní úpravy, a že je tento problém řešitelný vcelku úspěšně teoreticky**. Literatura i praxe se navíc shodly, že za listinu lze považovat (kromě běžných listin papírových) jakékoliv jiné hmotné médium (např. kůra, kámen či hliněná tabulka) na něž lze zachytit písemný projev, příp. cokoliv jiného, na čem může být písmo zachyceno s tím, že je lhostejno, „na jaké látce a jakou látkou"[6] je projev vůle sepsán (tedy např. text zachycený rytbou na bronzovou

[1] Článek vznikl na základě grantu uděleného GA AV ČR, registrační číslo B7068203 s názvem „Úprava elektronického podpisu v právním řádu ČR" a grantu uděleného GA AV ČR, registrační číslo 407/02/0575 s názvem „Odpovědnost některých osob v souvislosti s útoky na nástroje elektronického podpisu a související postupy dle zákona č. 227/2000 Sb."
[2] Občanský zákoník č. 40/1964 Sb. v platném znění (dále jen občanský zákoník)
[3] Jako např. svoboda, vážnost, určitost a srozumitelnost právního úkonu, včetně právně způsobilého subjektu (§ 37 a násl. občanského zákoníku)
[4] Je však třeba mít v této souvislosti na paměti ustanovení § 40 odst. 4 občanského zákoníku, stanovící, že písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.
[5] Eliáš, K., Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. AD NOTAM, 1996, č. 3, s.53
[6] Krčmář, J., Právo občanské, díl V. – Právo dědické, Všehrd, Praha, 1930, s.22

sochu, příp. v písku na písečné pláži či na zahrádce z květin). Obecně lze tedy konstatovat, že „listinou“ se v našem právním řádu tedy rozumí **cokoliv psaného**. Dále je zde třeba souhlasit s J.Burešem a L.Drápalem[7], podle nichž „**teoretické spory kolem listiny nemají praktického významu**“.

Platnost písemné formy právního úkonu ale nepředpokládá pouhé zachycení obsahu právního úkonu v textu listiny, ale též existenci podpisu. Písemný projev může být platný až od okamžiku podpisu jednající osoby. Nedodržení písemné formy činí právní úkon neplatným. V tomto směru je však třeba podotknout, že písemná forma podmiňuje platnost právního úkonu, nikoliv však jeho dokazatelnost. Dojde-li proto ke ztrátě či zničení textu listiny, není vyloučeno domáhat se nároků z právního úkonu. Lze-li ovšem tento právní úkon i splnění formy dokázat jinak (např. svědky, apod.); u listinných cenných papírů, u kterých jsou práva inkorporována je ovšem situace zcela jiná.[8] Obdobně, jak je tomu v případě pojmu „listina“, neobsahuje náš právní řád legální definici pojmu „podpis“. To však již - na rozdíl od tohoto pojmu – přináší **řadu jak praktických tak i teoretických problémů.**

Jednak není příliš jasné, jak úplný podpis je z hlediska práva ještě dostatečný a jaký již nikoliv. Nejenom, že není zdaleka zřejmé, zda postačuje podpis typu „Váš otec“[9], příp. „Tvá žena Renáta“, ale ani nelze jednoznačně odpovědět na otázku, zda postačuje strojový či jinak mechanicky na listině vytištěný podpis (řetězec znaků typu: Max Mayer), příp. vlastnoruční podpis (lidově zvaný jako „klikyhák“), či zda je třeba uvést **skutečné a úplné jméno tak, jak je zapsáno v matrice a osobních dokladech jednající osoby** (tedy nejenom včetně jména a příjmení, ale také i titulů, případně bydliště, rodného čísla, apod.) .

Těžko však hledat jednoznačnou odpověď. S tím ale velmi úzce souvisí i jednotlivé skupiny (kategorie) podpisu užívané v našem právním řádu. Vyjma některých – spíše překladových nesrovnalostí[10] – lze totiž ze (striktně) právního hlediska rozlišovat:

- podpis[11]
- vlastnoruční podpis[12]
- ověřený podpis (ať již soudně, notářsky nebo úřadně)[13]
- elektronický podpis (včetně jeho vyšších forem, kterými se budeme zabývat dále)[14]

Dle mého soudu je nesporné, že každá z výše uvedených skupin splňuje znaky podpisu dle § 40 odst. 3. občanského zákoníku. Zákonodárce velmi často obligatorně vyžaduje **náležitost podpisu.** V řadě případů však zákon výslovně požaduje **vlastnoruční podpis**, v jiných případech - ať již notářsky, soudně nebo úředně - **ověřený podpis**.

---

[7] Bureš, J., - Drápal, L.., Občanský soudní řád. Komentář. Praha, C.H. Beck 1996, s.61

[8] Jehlička, O. - Švestka, J. - Škárová, M. a kolektiv, Občanský zákoník – komentář, C.H.Beck, Praha, 1999, s.172

[9] K tomu více Eliáš, K., Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. AD NOTAM, 1996, č. 3, s.55

[10] Jde zejména o pojmy „vlastní podpis“, „podpis vlastní rukou“ (např. čl. 3 odst. 1 sdělení č. 179/1996 Sb.), které považuji s ohledem na dikci jednotlivých ustanovení za synonymické pojmu „vlastnoruční podpis“. Dále s ohledem na § 74 zákona č. 358/1992 Sb. za variantu podpisu nepovažuji „podpis na listině, který osoba uznala za vlastní“ či jiné jeho obdoby.

[11] Pojem „podpis“ se - bez dalších adjektiv – vyskytuje v našem právním řádu ve více jak 1000 dokumentech v počtu větším než 2800 výrazů (z toho však pouhých cca. 330 výrazů se nachází v cca. 100 zákonných předpisech)

[12] Pojem „vlastnoruční podpis“ již bývá zákonodárcem výslovně užíván velmi zřídka. Lze hovořit pouze o několika desítkách výrazů.

[13] Viz např. zákon č. 358/1992 Sb., o notářích a jejich činnosti (dále jen notářský řád) v platném znění

[14] Viz zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (dále jen zákon), v platném znění

Podpis (bez dalších adjektiv) tedy - s ohledem na logickou právní argumentaci - lze považovat za pojem obecný (nejužší), jehož náležitost může být zásadně splněna jakoukoliv další (vyšší) formou podpisu.

Podpis notářsky (či jinak úředně) **ověřený** je v některých případech zákonem vyžadován **jako jakási nejvyšší forma podpisu**, která je výsledkem legalizace[15]. Takovýto podpis je např. vyžadován u všech smluv, na základě kterých jsou katastrálním úřadem vkládána vlastnická či jiná věcná práva k nemovitostem do katastru nemovitostí. S ohledem na zaměření tohoto článku - vyjma některých souvisejících otázek[16] - se již však úředně ověřenými podpisy dále zabývat nehodlám.

Vzhledem k samotnému zákonnému rozlišování jednotlivých skupin podpisů, lze **tam, kde není požadován výslovně podpis vlastnoruční** (příp. notářsky či jinak ověřený), **vystačit i se strojovým či jinak mechanicky na listině vytištěným podpisem.**[17] Je ovšem třeba respektovat omezení náhrady podpisu mechanickými prostředky pouze na případy, kdy je to obvyklé[18].

S ohledem na ustanovení poslední věty[19] § 40 odst. 3 občanského zákoníku a dalších norem je dále třeba nepochybně hovořit i o **podpisu elektronickém**.

III. Místo závěru

Plné zrovnoprávnění elektronické formy s formou listinou vyžaduje změnu nejenom desítek právních předpisů (zejména těch procesních – zde jsme vzhledem k posledním změnám v této oblasti na dobré cestě), ale také především změnu v myšlení celé řady osob, právními teoretiky a soudci počínaje, úředníky a běžným občanem konče.

Elektronický podpis je řešením, které nepochybně zefektivní řadu běžných činností, čímž se snad podaří odstranit některé problémy související se skutečností, že je stále větší poptávka po využívání elektronických médií i pro nejrůznější úkony, pro které je v dnešní době stále ještě vyžadována "papírová forma" včetně vlastnoručního podpisu. Na druhou stranu je třeba v elektronickém podpisu vidět pouze jakousi záruku bezpečné komunikace či kvalitní archivace dat a ne jakýsi výlučný lék na zrovnoprávnění tradičních forem (zejména notářsky či jinak úředně ověřených) komunikace s formou elektronickou.

Z pohledu práva je třeba považovat elektronický podpis (a zejména jeho vyšší tzv. zaručené formy) za jakousi formu elektronické obálky, která vzhledem k existenci zvláštní zákonné úpravy představuje právní institut, který nemusí (ale může) zároveň naplňovat zákonný požadavek podpisu.

---

[15] Legalizace podpisu je jednou z typických notářských činností (§ 74 notářského řádu); krom toho jsou úředním ověřováním podpisů oprávněny i některé orgány veřejné správy, které vedou matriku (zákon č. 41\1993 Sb.) a také obecní a jím naroveň postavené úřady, které sice matriku nevedou, ale byly touto činností pověřeny podle vyhlášky č. 138\1993 Sb.

[16] Vyjma problematiky ověřování elektronického podpisu, o které budeme hovořit dále.

[17] K tomu však srovnej rozdílný výklad: Eliáš, K., Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. AD NOTAM, 1996, č. 3, s.54, který se domnívá, že „podpis platí zpravidla jen tehdy za řádný, je-li vlastnoruční .“. I on však připouští určité výjimky.

[18] viz § 40 odst. 3 občanského zákoníku

[19] Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.

G. Pozvánka na BIN 2002

ICZ zakládá tradici konferencí o bezpečnosti

Odedávna patří k největším úskalím elektronického zpracování dat jejich bezpečnost. Problémem není pouze vývoj potřebných systémů, ale také jejich schopnost přizpůsobit se požadavkům nové legislativy. Tématice dopadu legislativních opatření do oboru bezpečnosti informačních a komunikačních systémů se bude věnovat konference BIN 2002, konaná letos 11. září v Praze.

První ročník konference BIN - Bezpečnost informací má ambice založit každoroční tradici setkávání odborníků v oboru, řešitelů i uživatelů, lidí z teorie i praxe. Cílem společnosti ICZ a.s., která je pořadatelem tohoto fóra, je vyhledávat a přinášet na konferenci aktuální témata, která pomohou sblížit pozice odborníků a pracovníků z řad především středního managementu. Půjde přitom o mnohem širší pohled než jsou pouze záležitosti počítačových systémů. Účastníci konference dostanou nejnovější a prakticky využitelný přehled událostí v oboru za poslední rok včetně praktických a okamžitě použitelných výsledků práce špičkových expertů z ČR i zahraničí.

K výběru přednášejících a obsahu příspěvků prvního ročníku BIN 2002 přistoupila pořádající společnost ICZ v duchu firemní filozofie mnohovrstevného přístupu k řešení bezpečnosti informací včetně schopnosti poskytnout jak služby strategického charakteru, tak konkrétní technická řešení. Na konferenci vystoupí Ing. Ondřej Felix, CSc., předseda představenstva Českého Telekomu, RNDr. Ivan Svoboda, CSc. ze společnosti Oracle, Ing. Jaroslav Mejstřík z ČNB, Mgr. Pavel Vondruška z Úřadu pro ochranu osobních údajů a JUDr. Ján Matejka z Ústavu státu a práva AV ČR. Mezi přednášejícími jsou samozřejmě také odborníci ze společnosti ICZ Ing. Pavel Staša, RNDr. Vlasta Jošková a RNDr. Vlastimil Klíma spolu s Ing. Tomášem Rosou, kteří se s účastníky mimo jiné podělí o aktuální poznatky ze srpnového světového setkání kryptologů v USA.

Více informací včetně možnosti elektronické přihlášky najdete na http://www.i.cz/bin2002

H. Letem šifrovým světem

1. Návrh vyhlášok k slovenskému zákonu č. 215/2002 Z.z. o elektronickom podpise - odborné pripomienkové konanie

Návrhy vyhlášok sú v rámci pripomienkového konania Národného bezpečnostného úradu k zákonu č. 215/2002 Z.z. o elektronickom podpise na odborné pripomienkovanie sprístupnené na internetovej stránke Národného bezpečnostného úradu – http://www.nbusr.sk

Zoznam návrhov vyhlášok:
1. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 Z.z. o používaní elektronického podpisu v obchodnom a administratívnom styku
2. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 z dd. mm. 2002 o dokumentácii certifikačnej autority
3. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 z dd. mm. 2002, o podmienkach pre bezpečné zariadenia na vytváranie elektronického podpisu a používania časovej pečiatky a spôsobu ich hodnotenia
4. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 z dd. mm. 2002 o podmienkach vyhotovovania a používania zaručeného elektronického podpisu a časovej pečiatky, ktorou sa vykonáva zákon Národnej rady Slovenskej republiky č. 984/2002 Z. z. o elektronickom podpise
5. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 z dd. mm. 2002, o kvalifikovaných certifikátoch a zoznamoch zrušených kvalifikovaných certifikátov, ktorou sa vykonáva zákon Národnej rady Slovenskej republiky č. 984/2002 Z. z. o elektronickom podpise
6. Návrh vyhlášky Národného bezpečnostného úradu č. xxx/2002 z dd. mm. 2002, o podmienkach poskytovania akreditovaných certifikačných služieb, ktorou sa vykonáva zákon NR SR č. 215/2002 o elektronickom podpise

Pripomienky k daným vyhláškam bolo možné posielať do 26. júla 2002 na e-mailovú adresu info@nbusr.sk.

---

2. Na domovské stránce sešitu Crypto-World byla zpřístupněna další **sekce : „Právní předpisy a standardy pro EP“** . V této sekci najdete stručný přehled zákonů, vyhlášek, norem, pseudonorem a dokumentů souvisejících s elektronickým podpisem. Pro větší přehlednost jsou členěny do pěti oddílů:
Ochrana osobních údajů, Elektronický podpis, Elektronické podatelny, Standardy ISVS související se standardem pro provoz elektronických podatelen, RFC .
Připravuje se šestý oddíl, který bude věnován příslušným odstavcům z jednotlivých právních předpisů, kde již bylo akceptováno použití elektronického podpisu (např. Zákon o podpoře výzkumu a vývoje č.130/2002 Sb., Soudní řád správní č. 150/2002, Vyhláška 178/2002 Sb. Ministerstva financí , Vyhláška 117/2002 Sb. Ministerstva životního prostředí, Úřední sdělení ČNB 5/2002 ...).
Tato sekce má sloužit k rychlé orientaci v právní problematice EP v ČR a zpřístupnit všechny relevantní dokumenty na jediném místě a ušetřit čas osobám, které tyto informace potřebují.

---

3. Na domovské stránce e-zinu (http://www.mujweb.cz/veda/gcucmp/) v sekci **„Elektronický podpis (kniha)“** mohou vlastníci knihy „Bosáková, Kučerová, Peca, Vondruška : Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů“ najít **opravu strany 106.** Na této straně si šotek v tiskárně opravdu zařádil a místo důležitého odstavce je pod příslušnou tabulkou zopakován text uvedený pod předchozí tabulkou.

Současně si touto cestou dovoluji připomenout, že v případě citace z této knihy (resp. použití celých odstavců) je „vhodné“ uvést zdroj ☺.

---

4. Zájemce o téma **„časová razítka“** jsem se pokusil „potěšit“ tím, že k minulému číslu Crypto-Worldu 6/2002 jsem si zažádal o časové razítko u známé americké firmy DigiStamp. Na domovské stránce http://www.mujweb.cz/veda/gcucmp/ je dostupný certifikát této firmy, který můžete získat ke každému časovému razítku a je zde uloženo i samotné časové razítko. Časové razítko je ve formátu IP Protector. Certifikát obsahuje tyto údaje: název firmy, která vydává časové razítko, jméno žadatele, název souboru, ke kterému se časové razítko vydává, otisk tohoto souboru ve formátu SHA-1, datum a čas (GMT) vytvoření časového razítka, digitální podpis časového razítka firmy DigiStamp.

Základní informace k časovým razítkům lze najít v RFC 3161 (2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol ‚TSP). Tuto normu můžete nalézt na domovské stránce Crypto-Worldu v sekci „Právní předpisy a standardy pro EP“ (viz. odstavec 2 této kapitoly).

---

5. Od zavedení možnosti **registrace k odběru e-zinu Crypto-World** přímo z domovské stránky tohoto sešitu (18.6.2002) využilo tento postup za jeden měsíc 31 zájemců. Počet registrovaných odběratelů tak dosáhl 350.

---

6. Téměř 40 % podniků kontroluje zaměstnancům e-maily

Z květnového výzkumu iMonitor B2B agentury Taylor Nelson Sofres Factum vyplývá, že v České republice téměř 40 % firem kontroluje e-mailovou korespondenci zaměstnanců. Z toho 17 % podniků elektronickou poštu kontroluje pravidelně, 12 % občas a 10 % zřídka. 58 % firem e-korespondenci nekontroluje. Přísněji podniky sledují surfování zaměstnanců na internetu. Tuto činnost monitoruje pravidelně 19 % firem, 19 % občas a 14 % zřídka. 42 procent podniků tyto aktivity zaměstnanců nesleduje. Výzkum byl proveden na vzorku 500 českých podniků s velikostí nad 20 zaměstnanců.

---

7. Firma Datakey dodává své čipové karty pro zabezpečení on-line podání obchodních dokumentů v některých evropských zemích. V tomto pilotním projektu bylo dodáno již deset tisíc čipových karet a čteček Datakey. Firma Datakey rozšiřuje své aktivity i v Kanadě. Ve druhém čtvrtletí tohoto roku dodala své čipové karty, čtečky a klientský software šestnácti tisícům uživatelů tří kanadských ministerstev.

Více naleznete na: http://www.datakey.com , http://www.tsoft.cz/cz/08/00/245.pdf , http://www.tsoft.cz/cz/08/00/246.pdf

---

8. Přehled některých akcí (do konce října 2002)

Workshop on Cryptographic Hardware and Embedded Systems 2002 (CHES 2002), August 13 – 15, 2002, Hotel Sofitel, San Francisco Bay (Redwood city), USA,
http://islab/oregonstate.edu/ches/program.html
(vynikajícím úspěchem je, že mezi přednášejícími jsou i zástupci z ČR a SR),
Sekce 2 – Finite Field and Modular Arithmetic – R.Lórenz (CTU Prague, CZ) a
Sekce 6 – RSA Implementation – V.Klíma a T.Rosa (ICZ, CZ)
Sekce 9 – Random Number Generation - V. Fischer (U Jean Monnet, FR)
and M. Drutarovsky (U Kosice, SL)).

Konference BIN 2002, 11. září 2002 , hotel Praha, pořadatel ICZ, http://www.i.cz/
(Jošková,Vondruška: Elektronický podpis prakticky)

The 6th Workshop on Elliptic Curve Cryptography (ECC 2002), September 23 – 25, 2002
University of Essen, Germany, http://www.cacr.math.uwaterloo.ca/

Mezinárodní konference "Současná budoucnost": e-služby, 26.-27.září 2002 , Praha, pořádá Asociace podnikatelek a manažerek ČR, záštita SPIS, http://www.apmcr.cz/
(Vondruška: Použití elektronického podpisu v podnikání,
Vondruška, Matejka, Holcman: panelová diskuse : Legislativní podmínky e-podnikání: výhody a úskalí)

The eBusiness and eWork Conference: 6.-8.října 2002, Praha, http://www.ebew.net/

Konference „Informační bezpečnost – teorie a praxe“, INVEX 2002, 7. – 8. října 2002, Brno, http://www.afcea.cz
(Pinkava : Elektronický podpis – trendy a standardy v EU
Bosáková : Zkušenosti Úřadu s aplikací zákona o EP a vyhlášky)

RSA Security Inc. presents RSA Conference 2002, 7 - 10 October 2002, Le Palais des Congres de Paris, France, Download the RSA Conference 2002, Europe Brochure (3.4Mb), http://www.rsa.com/ , http://www.rsaconference.net/paris/

Konference ECIIA –2002, Interní audit v procesu globalizace, 17. – 18.října 2002, Hotel Inter-Continental Praha, http://www.interniaudit.cz/

DATAKON 2002 , 19. - 22. 10. 2002, Hotel SANTON, Brno, http://www.datakon.cz/

2nd European Conference on e-Government, October 2002,
http://www.mcil.co.uk/2g-eceg2002-home.htm

Odborná konference IIR - Trendy IT SECURITY , 29. a 30. 10. 2002, Praha, hotel Crowne Plaza, http://www.konference.cz/ , http://www.iir.at/
(Matejka, Vondruška : Možné útoky na elektronický podpis)

9. O čem jsme psali v červenci a srpnu roku 2000 a 2001

Crypto-World 78/2000

Příloha :

10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha :

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

I. Závěrečné informace

1. Sešit

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

Články neprocházejí jazykovou kontrolou!

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

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