Moderní kryptografické algoritmy pro elektronický podpis

Ing. Jaroslav Pinkava, CSc.

AEC spol. s r.o.

1.Úvod

Cílem předloženého materiálu je uvést čtenáře do současného stavu problematiky elektronických podpisů. Zdůrazněny jsou zde aspekty uplatnění existujících norem a standardů (zejména s ohledem na Evropskou Unii). Jedná se např. o základní používanou terminologii ve vztahu k elektronickým podpisům, o volbu příslušných kryptografických algoritmů pro digitální podpis, formy elektronických podpisů při využívání tzv. časových značek a také o problematiku validace (certifikace) podpisových prostředků.

2. Elektronický a digitální podpis

Elektronický podpis:

Pojem elektronického podpisu se objevil teprve nedávno. Dle definice z evropské Směrnice jsou jím míněna *data v elektronickém tvaru, která jsou připojena či logicky asociována k jiným elektronickým datům a která slouží jako metoda autentizace*.

Digitální podpis:

Digitální podpis zajišťuje autentizaci. Je to (obecně řečeno) řetězec znaků, který určitým způsobem svazuje veřejný klíč a zprávu. Pouze osoba znající zprávu a odpovídající soukromý klíč mohla vytvořit tento řetězec. Kdokoli, kdo zná zprávu a veřejný klíč, může tento digitální podpis verifikovat.

Většina systémů s veřejným klíčem je pomalá. Provést podpis dlouhé zprávy proto může být pro uživatele časově náročnou operací. Řešení poskytují hashovací funkce, jejichž rychlost je srovnatelná se symetrickými šifrovacími algoritmy a je tedy výrazně vyšší než rychlost algoritmů pro systémy s veřejným klíčem. Strana vytvářející digitální podpis určité zprávy nejprve spočte hodnotu hashe této zprávy a podepíše (svým soukromým klíčem) pouze tento hash. Kdokoli, kdo chce ověřit tento podpis postupuje analogicky. Spočte hodnotu hashe podepsané zprávy a porovná ji z hodnotou získanou dešifrací podpisu veřejným klíčem podpisující strany. Tedy podepsaný hash lze považovat za určitý otisk prstu (fingerprint) autora zprávy. Délka samotného hashe je přitom obvykle výrazně kratší než délka celé zprávy a tedy také vytvoření digitálního podpisu tohoto hashe trvá podstaně kratší dobu než kdyby byl vytvářen podpis celé zprávy.

Digitální podpisy ve formě otisku lze rovněž s výhodou využít např. v situacích, kdy je nutné uchovávat velkou řadu ověřených souborů. Pro každý takovýto soubor je spočten jeho otisk (message digest), který je pak spolehlivě uložen. Pokud je třeba prokázat správnost příslušného souboru, stačí znovu spočítat hodnotu jeho hashe a porovnat ji s dříve uloženou hodnotou hashe. Hashovací funkce lze také použít pro důkaz skutečnosti, že v příslušném souboru nebyly provedeny žádné změny (neboť dokonce přidání či změna jediného znaku vede ke kompletní změně hodnoty hashe). Dále důležitou úlohu hrají hashovací funkce při vytváření tzv. digitálních časových razítek. Hodnotu hashe lze totiž zveřejnit bez kompromitace obsahu vlastního dokumentu. Důvěryhodná strana podepíše hash dokumentu a časovou značku svým soukromým klíčem, tím je později zaručeno, že dokument v příslušném čase již existoval.

Digitální podpis s obnovou zprávy:

Digitální podpis, který obsahuje dostatečné množství informací k tomu, aby z podpisu byla získána podepsaná zpráva. To eliminuje potřebu zasílat zprávu s podpisem.

Digitální podpis v dodatku ke zprávě:

Takový digitální podpis, který neobsahuje podepsanou zprávu. Zpráva je k podpisu přiložena.

Směrnice Evropské Unie pro elektronický podpis, která vstoupila v platnost na počátku tohoto toku má za cíl sjednocení přístupu členských zemí k této problematice. Je zaměřena nejen na vlastní podpisové prostředky, ale zabývá se široce i problematikou tzv. poskytovatelů certifikačních služeb. Kromě základního pojmu elektronického podpisu se v evropských dokumentech objevují také následující pojmy.

Zaručený elektronický podpis:

(a) je jednoznačně vázán na podepisující osobu;

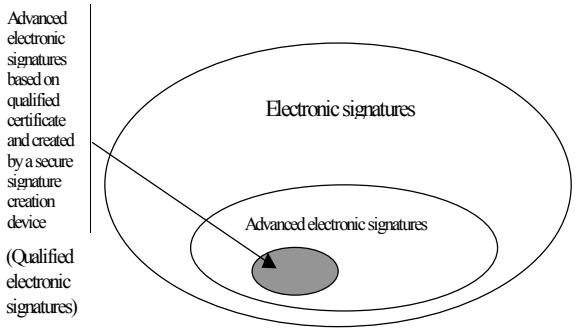
(b) umožňuje identifikaci podepisující osoby;

(c) je vytvořen prostředky, které podepisující osoba může mít pod svojí výhradní kontrolou;

(d) je vztažen k odpovídajícím datům takovým způsobem, že libovolná následná změna těchto dat je detekovatelná.

Kvalifikovaný elektronický podpis:

zaručený elektronický podpis založené na kvalifikovaných certifikátech a vytvořený pomocí prostředků pro bezpečné vytváření podpisu.



Obr.1.: Kvalifikované elektronické podpisy

(z dokumentu EESSI, lit.[1])

Následně vyjmenované mechanizmy, které vychází z mezinárodních norem a jsou veřejně dostupné, jsou doporučovány jako výchozí množina komponent, kterou lze použít pro kvalifikované elektronické podpisy:

- *Autentizace na bázi X.509 certifikátů [ISO/IEC 9594-8]*
- *X.509 PKI Certificate and CRL Profile [RFC 2459]*
- *Digitální podpisy na bázi algoritmů RSA a DSA [ISO/IEC 14888-1, -3]*
- *Hashovací funkce SHA-1 a RIPEMD-160 [ISO/IEC 10118-3]*
- *Cryptographic Message Syntax [RFC 2315] vycházející z veřejných specifikací (firma RSA) PKCS #7*
- *Použití hardwaru jako jsou čipové karty [ISO/IEC 7816 part 4-9, DIN Vornorm 6629 resp. RSA's specification PKCS#15], karty PCMCIA a Personal Digital Assistants (PDAs) pro bezpečné uložení a používání soukromých klíčů.*

3. Asymetrická kryptografie.

Historicky se objevuje pojem digitálního podpisu souběžně se vznikem asymetrické kryptografie v druhé polovině sedmdesátých let. Asymetrická kryptografie používá určitým způsobem propojenou dvojici kryptografických klíčů. Jeden klíč (veřejný) je používán k šifrování dat, druhý klíč (soukromý) slouží k dešifrování zašifrovaného obsahu dat. Přitom ze znalosti např. pouze veřejného klíče nelze odvodit hodnotu druhého (soukromého) klíče. Obecný princip (Diffie-Hellman, rok 1976), byl pak postupně realizován v řadě konkrétních kryptosystémů s veřejným klíčem. Kryptosystémy s veřejným klíčem umožňují přitom v zásadě trojí typ využití a to jako systémy pro:

- výměnu klíčů pro symetrickou kryptografii
- digitální podpis
- šifrování (obvykle krátkých zpráv, většinou služebního charakteru).

4. Mezinárodní normy

Existující mezinárodní normy pro oblast elektronických podpisů lze v zásadě roztřídit do tří základních okruhů. První z nich se týká použití hashovacích funkcí, druhý se týká samotných podpisových algoritmů. Konečně třetí okruh norem popisuje činnost v oblasti služeb tzv. třetích důvěryhodných stran a týká se, z hlediska terminologie použité v Směrnici EU pro elektronické podpisy, činnosti poskytovatelů certifikačních služeb. Podrobněji se lze s přehledem existujících norem seznámit ve zmíněném dokumentu EESSI [1].nebo v [11].

5. RSA

Tento algoritmus (1977) pro výměnu klíčů a tvorbu elektronického podpisu patřící mezi nejznámější. Jedná se o patentovanou (US Patent 4,405,829, 20.9.1983 vlastníkem je Public Key Partners (PKP), of Sunnyvale, California; patent vyprší po 17 letech, tj. letos - v roce 2000). RSA není patentován mimo Severní Ameriku. Na základě využívání RSA vznikla i známá americká společnost RSA Data Security Inc. Bezpečnost RSA je založena na skutečnosti, že je obtížné rozložit velká čísla (z nichž každé je součinem dvou velkých prvočísel), závisí tedy na možnostech řešit úlohu faktorizace.

Popíšeme stručně vlastní algoritmus:

Jednotliví uživatelé si vytváří dvojici veřejný a soukromý klíč pro RSA následovně:

a) nejprve náhodně (a nepredikovatelně – tato vlastnost je důležitá pro bezpečnost celého postupu) si vygenerují dvě dostatečně velká prvočísla **p** a **q** (jejich přibližná velikost tj. počet bitů je zadána)

b) Spočtou **n = pq** a **Φ = (p-1)(q-1)**.

Poznámka: stačí použít číslo **λ = NSN (p-1, q-1)**, tj. nejmenší společný násobek čísel **p-1** a **q-1**.

c) Zvolí náhodné číslo e, kde **1 < e < Φ**, tak, že **NSD (e, Φ) =1**. NSD značí největšího společného dělitele.

d) Užitím Eukleidova algoritmu spočte jednoznačně definované číslo **d** takové, že **1 < d < Φ**

a **ed ≡ 1 mod Φ** .

Veřejným klíčem je potom **(n,e)**, soukromým klíčem uživatele je **d**.

Popíšeme nyní jak probíhá vlastní šifrování a dešifrace. Předpokládejme, že strana B zná autentický veřejný klíč strany A, kterým je **(n,e)** a zašifrovává zprávu **M** pro A. Strana B vyjádří zprávu **M** jako číslo **m**, **0 ≤ m ≤ n-1** (resp. posloupnost takových čísel). Dále strana B spočte

$$c = m^e \bmod n$$

a zašle šifrový text straně A. Strana A nyní při dešifraci spočte pomocí soukromého klíče **d**

$$m = c^d \bmod n$$

Existuje několik variant podpisových schémat na bázi RSA. V současné době jsou nejvíce používany podpis vycházející z finanční normy ANSI X9.31 a podpisové schéma na bázi nové verze PKCS #1 v2.1: RSA Cryptography Standard, která vznikla již v návaznosti na dokumenty skupiny IEEE P1363.

RSA je součástí řady dalších oficiálních norem. Norma ISO 9796 (International Standarts Organization) bere RSA jako kompatibilní kryptografický algoritmus, stejně tak Norma CCITT X.509 (Consultative Committee in International Telegraphy and Telephony). Je součástí normy SWIFT (Society for Worldwide Interbank Financial Telecommuni-cations), normy ETEBAC 5 francouzského finančního průmyslu a normy ANSI X9.31 pro americký bankovní průmysl. Australská norma pro správu klíčů AS2805.6.5.3 rovněž specifikuje RSA.

Blízkým k systému RSA je Rabin-Williamsův systém. Jeho bezpečnost je stejně jako u RSA odvozována z obtížnosti řešení úlohy faktorizace velkých čísel. Stejně jako RSA je i Rabin-Williamsův kryptosystém součástí materiálů pracovní skupiny IEEE P1363 a je tedy jedním ze systémů, které jsou jako součást mezinárodních norem využitelné pro širší praktické aplikace.

6. DSA

DSS značí Digital Signature Standard, který specifikuje Digital Signature Algorithm (DSA). Byl vybrán NIST (ve spolupráci s NSA) jako vládní norma pro digitální autentizaci. Tato norma (FIPS – 186) původně obsahovala jediný algoritmus, který je založen na problému diskrétního logaritmu a je odvozen ze systému, který původně navrhli Schnorr a ElGamal.

Algoritmus obsahuje následující parametry:

1. p = prvočíslo, kde $2^{L-1} < p < 2^L$

pro $512 \le L \le 1024$ a L je násobek 64

2. q = prvočíslo, dělitel p - 1, kde $2^{159} < q < 2^{160}$

3. $g = h^{(p-1)/q} \bmod p$, kde h je libov. přirozené číslo, pro které $1 < h < p - 1$ a takové, že $h^{(p-1)/q} \bmod p > 1$

(g je řádu q mod p)

4. x = náhodně resp. pseudonáhodně generované celé číslo $0 < x < q$

5. $y = g^x \bmod p$

6. k = náhodně resp. pseudonáhodně generované celé číslo $0 < k < q$

Přirozená čísla p, q a g mohou být zveřejněna a mohou být společná pro skupinu uživatelů. Soukromým klíčem uživatele jsou x resp. y.Tato čísla jsou obvykle neměnná pro určité časové období. Parametry x a k jsou používánapouze pro generování podpisu a musí být utajována. Parametr k musí být pro každý podpis znovu generován.

Generování podpisu

Podpis zprávy M tvoří dvojice čísel r a s, která je spočtena následovně:

$r = (g^k \bmod p) \bmod q,$

$s = (k^{-1} (\text{SHA-1}(M) + xr)) \bmod q.$

Ověření podpisu

Zde M´, r´, a s´ jsou obdržené verze M, r, a s, a y je veřejný klíč podepisující strany. Nejprve ověřující strana zjistí zda platí $0 < r´ < q$ a $0 < s´ < q$. Potom spočítá

$w = (s´)^{-1} \bmod q$

u1 = ((SHA-1(M´))w) mod q

u2 = ((r´)w) mod q

v = (((g)^{u1} (y)^{u2}) mod p) mod q.

If v = r´, je podpis ověřen.

Algoritmus je určen pouze k autentizaci. Po svém zveřejnění byl algoritmus poměrně značně kritizován, zejména z následujících důvodů: chybí prostředky pro výměnu klíčů, o bezpečnosti příslušného kryptosystému se zatím ví poměrně málo, verifikace podpisů pomocí DSA je pomalá, byl očekáván standart na bázi RSA. V systému DSA je generování podpisu rychlejší než verifikace tohoto podpisu, u RSA je to obráceně (při vhodné volbě veřejného a soukromého exponentu), řada odborníků se domnívá, že je lépe, když rychlejší je verifikace.

Nejvíce však byl algoritmus kritizován z hlediska jeho bezpečnosti. Původní návrh obsahoval délku použitého prvočísla 512 bitů. Po široké kritice provedl NIST revizi návrhu a prodloužil tuto délku na 1024 bitů. I když úloha diskrétního logaritmu má již svou historii, její speciální verze použitá v DSS byla poprvé navržena Schnorrem v roce 1989. DSS je úřadem NIST patentována.

V posledních dvou letech prošla norma DSS dvojí reedicí. Koncem roku 1998 (FIPS 186-1) zde byl doplněn algoritmus RSA (dle formulace z normy ANSI X9.31) a v lednu tohoto roku (FIPS 186-2) byla norma doplněna celou sadou eliptických křivek. Kupodivu, přestože se o tom v odborných kruzích hodně diskutovalo, nebyla prodloužena délka prvočísla u základního algoritmu (předpokládalo se, že vzroste z 1024 bitů na 2048 bitů).

7. ECDSA

Pro realizaci eliptických kryptosystémů jsou využívány především dva základní typy těles. Jednak to jsou tělesa prvočíselná (operace probíhají mod p, kde p je prvočíslo), jednak jsou to tělesa binární (resp. se jim také říká tělesa charakteristiky dva - operace probíhají mod 2^n, n je přirozené číslo – dnes je doporučováno používat jako n rovněž pouze prvočísla).

Existuje několik schemat podpisu, která se opírají o použití eliptických kryptosystémů. Jako příklad uvedeme snad nejpoužívanější z nich (je to vlastně varianta DSA užitá v jiném tělese).

Generování podpisu.

Vstupy:

1. Zpráva M libovolné délky.

2. Parametry eliptické křivky q, a, b, bod P=(x_p,y_p) a prvočíslo n.

3. Soukromý klíč d.

Zpracování zprávy:

Spočteme hash e = H(M) pomocí SHA-1 (celé číslo v délce 160 bitů)

Výpočty na eliptické křivce:

1.Generování náhodného k, 1 < k < n.

2. Spočtení bodu na eliptické křivce (x_1,y_1) = kP.

3. Převedení x_1 na celé číslo x_1´.

4. Položíme r = x_1´ mod n..

5. Je-li r=0, jdeme zpět ke kroku 1.

Modulární výpočty:

1. Spočteme s = k^{-1} (e + dr) mod n
2. Pokud s=0 jdeme na krok 1. předešlého oddílu.

Podpis: Je jím dvojice (r,s) výše spočtená.

Ověření podpisu:

Vstupy:

1. Získaná zpráva M.

2. Získaný podpis zprávy M - dvě celá čísla r´ a s´ .

3. Parametry eliptické křivky q, a, b, bod P=(x_p,y_p) a prvočíslo n.

4. Veřejný klíč Q.

Zpracování zprávy:

Spočteme hash e = H(M) pomocí SHA-1 (celé číslo v délce 160 bitů)

Výpočty na eliptické křivce:

1. Pokud r´není v intervalu od 1 do n-1, podpis zamítneme

2. Pokud s´není v intervalu od 1 do n-1, podpis zamítneme

3. Spočteme $c = (s´)^{-1} \bmod n$.

4. Spočteme $u_1 = ec \bmod n$ a $u_2 = r´c \bmod n$.

5. Spočteme bod na eliptické křivce $(x_1,y_1) = u_1P + u_2Q$

Ověření podpisu:

1. Převedeme x_1 na celé číslo $x_1´$.
2. Spočteme $v = x_1´ \bmod n$.
3. Pokud $r´ = v$, pak je podpis ověřen.

Existuje několik variant podpisových schémat, která se opírají o využití eliptických kryptosystémů. Výše popsaný postup je označován jako

- EC-DSA .

Další varianty jsou v literatuře označovány jako

- EC-GDSA

(El-Gamal)

- EC-NR

(Nyberg-Rueppel)

- EC-KCDSA

(korejská varianta, tzv. prokazatelně bezpečná)

Kryptosystémy na bázi eliptických křivek vzhledem k možnosti volit z obrovského množství parametrů pro tyto křivky jsou velmi bohatým zdrojem algoritmů pro digitální podpisy. Tento fakt je na relativně velmi výhodný. Avšak na druhou stranu při praktických realizacích jsme nuceni omezit se na určitou konkrétní volbu parametrů (jinak by se jednotliví uživatelé nedomluvili). Za tímto cílem proběhl o v poslední době několik iniciativ (ANSI, SECG, NIST), vesměs sledujích určitá doporučení, tj. navrhují volit určité konkrétní hodnoty parametrů eliptických kryptosystémů. Je zde uplatňováno i určité bezpečnostní hledisko, parametry jsou voleny tzv. prokazatelně náhodně. Také v nové normě DSS (FIPS – 186-2) jsou definovány již určité hodnosty parametrů pro eliptické křivky, tyto hodnoty jsou vzájemně odlišené jednak typem příslušného tělěesa (binárního, prvočísleného), jednak délkou použitého prvočísla (resp. počtem bodů příslušné eliptické křivky).

8. Ostatní systémy a přístupy

Protože pro dnešní praktické aplikace má smysl uvažovat pouze systémy, které jsou předmětem určitých norem, standardů, lze říci, že výše uvedené tři rodiny algoritmů (IF – integer factorization, DL – discrete logarithm, EC – elliptic curves) v zásadě vyčerpávají dnešní hlavní přístupy k řešení digitálních podpisů na bázi asymetrické kryptografie. Přesto stojí za zmínku ještě dvě takové rodiny. Jsou to systémy označované NTRU, které jsou již součástí pokračujících prací skupiny IEEE P1363 a na letošním hlavním pracovním zasedání P1363 bude předložen německý návrh k obdobnému zařazení kryptosystémů, které využívají aritmetiku v tzv. kvadratických tělesech.

V posledních dvou letech je pozornost teoretiků obrácena k tzv. prokazatelně bezpečným kryptosystémům s veřejným klíčem. Varianty těchto kryptosystémů se samozřejmě objevují i pro oblast digitálních podpisů a není vyloučeno, že se s nimi setkáme i v blízké praxi. Nejedná se o zcela nový přístup k základním kryptografickým algoritmům, jako jsou např. algoritmy na bázi diskrétního logaritmu, ale jedná se více méně o práci s těmito algoritmy, o doprovodné protokoly atd. Moderní modifikace klasických kryptosystémů (Shoup, Pointcheval) mají zajistit dosažení vyšší úrovně bezpečnosti při zhruba stejné výpočetní efektivnosti implementací.

Mimo rámec tohoto přehledu zůstaly také různé speciální varianty digitálních podpisů (blind signatures, fair-stop signatures, undeniable signatures, group signatures, threshold signatures, atd.), které jsou používány pro řešení určitých specifických situací.

9. Používané hashovací funkce

Vstupem (jednosměrné) hashovací funkce je blok proměnné délky (zpráva) a výstupem je blok pevné délky (obvykle 128 či 160 bitů) – hash. Při dané hodnotě hashe je výpočetně nemožné najít zprávu s tímto hashem, ve skutečnosti na základě znalosti hashe zprávy nemůžeme nic říci o obsahu vlastní zprávy. Pro používané jednosměrné hashovací funkce je rovněž výpočetně nemožné najít dvě různé zprávy s touž hodnotou hashe.

SHA-1:

SHA-1 (Secure hash algoritnm) je hashovací funkce odpovídající normě FIPS PUB 180-1.Vytvoří 160 bitů dlouhý kontrolní hash. Algoritmus byl vyvinut NIST jako součást SHS (Secure Hash Standard). Původně publikovaný algoritmus SHA byl stažen a toto je jeho opravená verze. Algoritmus je zhruba o 25% pomalejší než MD5 (je však svým způsobem bezpečnější, poskytuje delší hodnotu hashe – 160

namísto 128 bitů). Byl navržen v souvislosti s normou DSS (Digital Signature Standard).

MD5:

Algoritmus MD5 vyvinula společnost RSA Data Security Inc. Lze ho použít k vytvoření hashe v délce 128 bitů ze zprávy libovolné délky. Je považován za dostatečně bezpečný algoritmus a je široce používán. Avšak např. Hans Dobbertin ukázel, že pro kompresní funkci MD5 lze nalézt kolize zhruba za 10 hodin na PC. Pokud však tento typ útoku nebude rozšířen na plnou verzi MD5 nelze pochybovat o bezpečnosti algoritmu. MD5 je veřejně dostupný k libovolnému použití.

RIPEMD-160:

Novějším hashovacím algoritmem je RIPEMD-160, který byl navržen s cílem nahradit MD4 a MD5. Vytváří (jak vyplývá z jeho názvu) hash v délce 160 bitů. Byl vyvinut v rámci evropského projektu RIPE. Úplný popis RIPEMD-160 lze nalézt například na adrese http://www.esat.kuleuven.ac.be/~bosselae /ripemd160.html.

10. Digitální certifikáty

Uživatelé musí být schopni získat bezpečnou cestou klíče, které potřebují k zašifrovaní svých dat. Pro systémy s veřejným klíčem zde musí být cesta, jak se podívat, jaký veřejný klíč používá druhá strana. A na druhé straně musí mít cestu ke zveřejnění svého klíče. To ale nestačí. Uživatel musí mít důvěru v legitimnost takto získaného klíče. V opačném případě by mohl narušitel buď zaměnit veřejný klíč ležící někde v adresáři nebo by se mohl vydávat za někoho jiného. Pro tyto účely slouží certifikáty. Digitální certifikát označuje vlastníka veřejného klíče. Dovoluje verifikaci tvrzení, že daný veřejný klíč patří skutečně danému jedinci. Certifikáty pomáhají chránit se před možností, že někdo falzifikuje klíč s cílem vydávat se za někoho jiného. Ve své nejjednodušší podobě obsahují certifikáty veřejný klíč a jméno. Obecně užívané certifikáty obsahují rovněž:

- dobu vypršení platnosti
- jméno certifikační autority, která vydala certifikát
- pořadové číslo
- informaci o tom jak klíč má být používán
- digitální podpis vydavatele certifikátu

Certifikáty nesmí být možné padělat, musí být získány bezpečnou cestou a vytvářeny musí být tak, aby potenciální narušitel je nemohl zneužít. Vydání certifikátu musí rovněž probíhat bezpečným způsobem, musí být odolné proti možným útokům. Pokud by něčí soukromý klíč byl ztracen či kompromitován, pak ostatní uživatelé musí být včas varováni a nesmí již déle šifrovat zprávy neplatným veřejným klíčem nebo akceptovat zprávy podepsané tímto zkompromitovaným soukromým klíčem. Uživatelé musí své klíče mít bezpečně uloženy, na druhé straně musí mít tyto klíče k dispozici pro jejich legitimní používání. Klíče mají platit pouze do doby než vyprší jejich platnost. Doba platnosti musí být vhodně zvolena a bezpečně opublikována. Je třeba rovněž vzít do úvahy, že některé dokumenty budou mít zapotřebí ověřit platnost podpisu i po uplynutí doby platnosti daného veřejného klíče.

Nejrozšířenějším akceptovaný formát pro certifikáty je definován mezinárodní normou CCITT X.509. Tyto certifikáty mohou být pak čteny či psány libovolnou aplikací vytvořenou ve shodě s X.509.

Problematika digitálních certifikátů a navazujících pojmů (kvalifikované certifikáty, certifikační autority atd.) je dnes již velice širokou oblastí problematiky a to oblastí nesmírně potřebnou zejména z hlediska praxe elektronických podpisů.

11. Formy elektronických podpisů

Evropští odborníci dnes rozpracovávají problematiku Směrnice Evropské Unie do celé řady koncepčních a normativních dokumentů. Příkladem může být dokument ([5]) ETSI, který se nazývá „Forms of Electronic Signature“. V zásadě se jedná o hlubší detailizaci pohledu na elektronické podpisy opírající se o využívání časových značek (time-stamping).

Dokument např. rozlišuje tři základní formy elektronických podpisů:

- Basic Electronic Signature (BES), tato forma zahrnuje digitální podpis a případnou další informaci, kterou poskytla podepisující osoba.
- Partial Electronic Signature (PES), tato forma přidává časovou značku a další informace (např. Certifikáty) k BES, tak aby byly učiněny výchozí kroky k dlouhodobé platnosti podpisu
- Complete Electronic Signature (CES), tato přidává k PES kompletní sadu dat, která podporují platnost elektronického podpisu (např. informaci, která se dotýká případného zneplatnění všech použitých certifikátů).

Například podepisující strana musí použít nejméně formu BES, v některých případech se může rozhodnout pro PES a v extrémních případech může použít formu CES. Pokud podepisující strana nepo-

užila PES, pak ověřující strana musí při prvním příjmu elektronického podpisu PES vytvořit. Pokud CES forma nebyla vytvořena již podepisující stranou, pak ověřující strana musí CES vytvořit jakmile jsou k dispozici data ve vztahu k revokacím, resp. jiná ověřovací data.

12. Bezpečnost kryptografických metod a potřebné délky klíčů

Velice důležitá součást problematiky, pro nedostatek místa však není možné ji zde obsáhnout v potřebné šíři. Čtenáře zainteresované problematikou bezpečnosti kryptosystémů s veřejným klíčem odkazuji na webovské stránky firem RSA Data Security (např. známý dokument labsfaq, nyní verze 4), Certicom resp. na stránky pracovní skupiny IEEE P1363. Na webu lze také nalézt dlouhou řadu článků různých autorů, které se danou problematikou v různých souvislostech zabývají.

Úzce s tím souvisí i otázka vhodné délky klíče pro uvedené kryptosystémy. Zde bych z poslední doby doporučil článek Arjen K. Lenstra; Eric R. Verheul : Selecting Cryptographic Key Sisez, November 1999, který lze nalézt na adrese http://www.pwcglobal.com/cce.

13. Validace (certifikace) bezpečných kryptografických prostředků

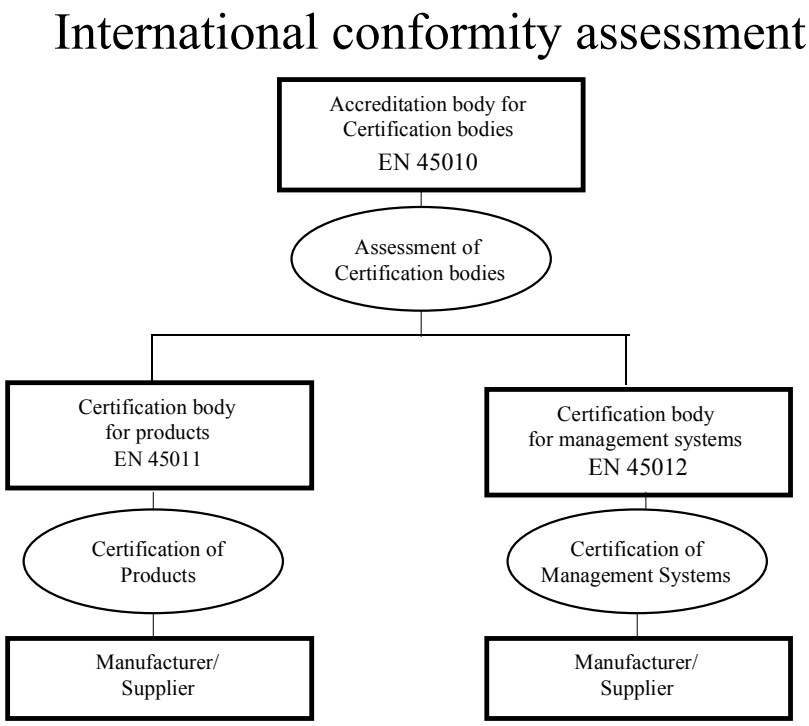
Příloha III (Annex III) Směrnice EU pro elektronický podpis se zabývá požadavky, které by měl splňovat tzv. bezpečný podepisovací prostředek. Je předpokládáno, že bude zpracována adekvátní norma, která detailně tyto požadavky rozpracuje. Určování shody (ať již dobrovolnou certifikací či deklarací výrobce) pak bude prováděno vzhledem k této normě.

V současné době nejvíce užívanou a všeobecně akceptovanou technologií pro implementaci bezpečného podepisovacího prostředku jsou čipové karty společně s příslušnou čtečkou čipových karet. Čipová karta obsahuje „data pro vytváření podpisu“, tj. soukromý kryptografický klíč, který je podepisující osobou použit při vytváření elektronického podpisu. Tato data jsou ještě chráněna PIN kódem. Soukromý klíč nemůže být přečten, a blokovací funkce chrání PIN karty proti provedení “totálních zkoušek“, tudíž čipovou kartu nelze okopírovat. Obdobnou úroveň bezpečnosti mohou poskytnout analogická hardwarová zařízení, jako karta PCMCIA, mobilní telefon se SIM kartou resp. tzv. Personal Digital Assistant.

V přítomné době jsou k ochraně soukromého klíče obvykle používány PIN či heslo. Předpokládá se, že v budoucnu by pro tyto účely mohly být využívány biometrické identifikační prostředky (speciálně např. otisky prstů).

Odborníci se ještě nedohodli, zda k ochraně soukromého klíče (tak, aby byly splněny požadavky přílohy III Směrnice EU) stačí ochrana v softwaru PC nebo zda jsou nutné výše uvedené hardwarové prostředky. V současné době je pouze konstatováno, že pokud jsou tyto hardwarové prostředky použity, pak požadavky přílohy III. mohou být splněny snadněji.

Normy EN 45010, EN 45011 a EN 45012 specifikují cesty akreditace institucí, které se hodlají zabývat certifikací výrobků a řídících systémů. Tyto normy jsou rovněž opublikovány ISO/IEC jako tzv. Guides 61, 66 a 62. V Evropské Unii má každý členský stát příslušnou akreditační instituci, která je v tomto státě uznávána a provádí tyto akreditace (např. SWEDAC, COFRAC, UKAS, RvA).



Obr.2.: Mezinárodní určování shody (EESSI)

Akreditovaná certifikační instituce provádí určování shody a certifikaci organizací dle specifických norem z příslušné oblasti (funkčnost, oblast řízení, kvality, technická). Evropská spolupráce pro oblast akreditace napomáhá vzájemnému uznávání provedených certifikací.

Z hlediska elektronických podpisů je požadována shoda v oblasti kvalitativních, řídících a funkčních aspektů. Předpokládá se, že budou rozpracovány příslušné normy, oproti kterým bude příslušná shoda určována. Zatím rovněž nejsou zpracována kriteria, podle kterých by měla probíhat akreditace certifikačních institucí. Na základě požadavku EESSI by tato kriteria měla být v nejbližší době zpracována.

Je doporučováno, aby akreditace certifikačních institucí probíhala v Evropském společenství jednotně a to v rámci Evropského akreditačního schématu dle EN 45010. Tato cesta významně napomůže vzájemenému uznávání certifikovaných produktů mezi jednotlivými státy společenství.

14. Závěr

Cílem předložených poznámek bylo provést určitý přehled v oblasti normativních postupů vzhledem k problematice elektronických podpisů v rámci Evropské Unie. Vzhledem k tomu, že tato oblast je v současné době předmětem bouřlivého rozvoje nelze provedený přehled považovat zdaleka za úplný. Autor bude proto považovat za úspěch pokud se mu podařilo upozornit alespoň na některé ze stěžejních evropských dokumentů v oblasti norem, které se vztahují k elektronickým podpisům.

Literatura

[1] Final Report of the EESSI Expert Team 20th July 1999, http://www.ict.etsi.org/eessi/Final-Report.doc

[2]http://europa.eu.int/comm/dg15/en/media/sign/index.htm Směrnice EU pro elektronický podpis

[3]http://www.ict.etsi.org/eessi/EESSI-homepage.htm

evropské dokumenty

[4] Draft ES 200 000 V0.8b (1999-08-02), Electronic signature standardization for business transactions

[5] Draft ETSI ES 201 733 V1.1.4 (1999-11-25) Electronic Signature Formats

[6] http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm

přehled existujících legislativních iniciativ v oblasti digitálních (a elektronických) podpisů v celém světě.

[7] Jaroslav Pinkava: Úvod do kryptologie, květen 1998, http://www.aec.cz

[8] Jaroslav Pinkava: Elektronický podpis a EU, DSM 2/2000

[9] Österreichisches Datenschutzgesetz z 13.7.99

rakouský zákon o elektronickém podpisu

http://www.dud.de/dud/dudstart.htm#Aktuelles

[10] Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigGÄndG), 6.1.2000 – výchozí formulace k návrhu nového německého zákona o elektronickém podpisu

http://www.dud.de/dud/dudstart.htm#Aktuelles

[11] J. Pinkava: Digitální a elektronický podpis ve světě a v EU. Legislativní a standardizační aspekty. Seminář AFOI, únor 2000

[12] IEEE P1363 - Standard Specifications for Public-Key Cryptography.

[13] ANSI X9.62: Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA).