Elektronické podpisy a Evropská Unie.

Koncem minulého roku byla Evropským Parlamentem schválena Direktiva EU pro elektronický podpis. Jaký je její smysl, co je jejím obsahem? A co Česká republika? Co vše je třeba udělat, abychom mohli prakticky používat elektronické podpisy? Na tyto a příbuzné otázky se pokusí odpovědět předkládaný článek.

Význam podpisu

Než se začneme probírat současnou terminologií v oblasti elektronických podpisů obraťme se nejprve ke klasického pojmu **podpis** a trochu si ho rozeberme. K samotnému podpisu vždy patří nějaký určitý dokument, materiál, který jsme podepsali, nebo který právě podepisujeme. V zásadě lze říci, že podpis na dokumentu vytváří určitou situaci, která je dále již nevratná. Podpisem je obvykle jednoznačně označena osoba, která daný dokument podepsala. Dále pak z vlastní povahy podepsaného dokumentu vyplývá konkrétní smysl (účel) samotného podpisu. Podepisující osoba podpisem dokumentu např.:
- poskytuje důkaz, že se cítí být obsahem dokumentu (smlouvy) vázána;
- podepsaný dokument může sloužit jiné straně jako věrohodná záruka pro splnění určitých závazků (peněžních, hmotných, časových atd.), přitom význam těchto závazků je v dokumentu popsán;
- stvrzuje autorství textu dokumentu, jestliže podepsaný dokument sepsal někdo jiný, pak podepisující osoba potvrzuje svůj úmysl ztotožnit se s obsahem daného dokumentu;
- prokazuje skutečnost, že tato osoba byla přítomna na stanoveném místě (a např. v danou dobu), podepisující se strana pak může tento podpis využít k prokázání této přítomnosti.

Z hlediska právní podstaty je podpis „stvrzením právního úkonu provedeného v písemné formě“". Podepisující osoba vyjadřuje svým podpisem svoji ochotu potvrdit závazky vyplývající z podstaty dokumentu. Pro tyto účely je podpis používán vzhledem k tomu, že je jednoduše proveditelný, srozumitelný, snadno se s ním operuje a poměrně nesnadno je zneužitelný. Zejména z hlediska těchto vlastností zaujal také podpis své místo v historické praxi vytváření závazných dokumentů.

V současné době se však i díky moderním technologiím význam tohoto klasického podpisu začíná zmenšovat. Dokumenty cestují v elektronické podobě (oskenované, faxem) a není příliš obtížné padělat na obrazové (faxové) variantě dokumentu ručně psaný podpis. Přitom elektronických dokumentů stále přibývá a uživatelé si uvědomují výhodnost takového pohybu dokumentů. Je však třeba najít jinou cestu k podepisování takovýchto dokumentů. Musí to být postup, zaručující určité vlastnosti, které podepsaný dokument získá. Strana, která získá podepsaný dokument bude samozřejmě chtít být ubezpečena, že autorem dokumentu je označená osoba, že se seznamuje s přesným obsahem dokumentu, že může na základě takto získaného dokumentu konat a mít přitom určité záruky od autora dokumentu.

Jinými slovy je třeba zajistit u těchto dokumentů jejich ***autentičnost*** (původ, autora), jejich ***neporušenost*** (integritu), ale i tzv. ***nepopiratelnost*** (podepsaná strana nemůže později popřít, že daný dokument podepsala). Ještě je třeba poznamenat, že za některých okolností k tomu přistupují i nároky na ***utajení*** obsahu dokumentu před nepovolanou osobou – v našem článku se však těmito otázkami zabývat nebudeme.

Digitální podpis

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. Nejznámějším (a zřejmě i v současnosti nejpoužívanějším) je **RSA**, kryptosystém založený na obtížnosti úlohy faktorizace velkých čísel. Kromě tohoto modelu jsou dnes rovněž používány kryptosystémy s veřejným klíčem založené na úloze diskrétního logaritmu resp. eliptického diskrétního logaritmu. Kryptosystémy s veřejným klíčem jsou dnes používány pro řešení tří následujících okruhů problematik: ***výměna klíčů*** (pro symetrickou kryptografii), ***šifrování*** (krátkých zpráv, většinou služebního charakteru) a pro ***digitální podpisy***. V tomto článku nás samozřejmě zajímá především zmíněné třetí využití těchto kryptosystémů. Kromě RSA jsou dnes používána podpisová schémata **DSA** (původní americká norma pro digitální podpis) a **ECDSA** (moderní varianta, založená na využití eliptických křivek).

Digitální podpis je tedy pojem vycházející z použití kryptosystémů s veřejným klíčem. Jak probíhá pro určitý dokument vytváření jeho digitálního podpisu (např. autorem)? Nejjednodušší přístup je následující (*digitální podpis s obnovou zprávy*): Podepisující strana vezme příslušný dokument v elektronické podobě a zašifruje ho svým soukromým klíčem. Vhodnou cestou přitom zveřejní (nebo již má zveřejněn) odpovídající veřejný klíč. Kdokoliv, kdo má přístup k tomuto veřejnému klíči (a ověří si, kdo je jeho skutečným majitelem), může nyní pomocí tohoto veřejného klíče dešifrovat podepsaný dokument a ověřit tak příslušný podpis tohoto dokumentu.

Obvykle je však volen trochu složitější přístup. Je to proto, že kryptosystémy s veřejným klíčem oproti klasickým kryptosystémům mají jednu méně příjemnou vlastnost – jsou význačně pomalejší. Nejsou proto vhodné pro šifrování zpráv o delším rozsahu. Abychom však mohli podepisovat i takovéto delší zprávy, využíváme tzv. hashovací fukce. Pomocí hashovací funkce je z původní zprávy vyroben její tzv. otisk (message digest) – má relativně krátkou délku, obvykle 160 resp. 128 bitů. Teprve tento otisk zprávy je pak podepisován příslušným soukromým klíčem. Podpis tohoto hashe je pak připojen k vlastní podepisované zprávě (proto se také tomuto postupu při podepisování říká *digitální podpis v dodatku zprávy*). Ověření takového podpisu probíhá v zásadě analogicky jako v prvním případě, pouze je třeba nejprve opět spočíst k dané zprávě její hash.

K tomu, abychom např. výše zmíněné systémy (RSA, DSA, ECDSA) mohli používat jako adekvátní podpisová schémata, je nezbytné mít velice důkladně prozkoumány příslušné kryptografické vlastnosti daných algoritmů, zejména z hlediska nutnosti zajistit jejich bezpečné používání. Například je nutné stanovit požadovanou minimální délku klíče (počet jeho bitů), jedná se však i o posouzení odolnosti schémat proti celé řadě velice různorodých útoků.

Důležitým souvisejícím pojmem je pojem ***digitálního certifikátu*** příslušného veřejného klíče. 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 existovat cesta ke zveřejnění vlastního veřejného 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 a asociuje vlastníka a veřejný klíč. Dovoluje verifikaci tvrzení, že daný veřejný klíč patří skutečně danému jedinci. Certifikáty pomáhají chránit uživatele před možností, že někdo falzifikuje klíč s cílem vydávat se za někoho jiného.

Úkol zveřejnit digitální certifikáty důvěryhodnou cestou na sebe přebírá speciální instituce – ***certifikační autorita*** (CA). Certifikační autorita na základě žádosti o certifikát (doplněné předloženými dokumenty dle obsahu certifikátu – např. občanským průkazem, atd.) vydá příslušný certifikát, který je podepsán soukromým podpisovým klíčem dané CA. CA zároveň zabezpečuje potřebné zveřejnění takto vzniklého certifikátu (v příslušném adresáři, který může, ale nemusí, být veřejně přístupný). Zajišťuje také funkčnost seznamu revokovaných (zneplatněných – např. z bezpečnostních důvodů) certifikátů – CRL. Další podrobnosti lze nalézt např. v [2].

obr. 1.: Certifikát CA

Elektronický podpis

Obecnějším pojmem než digitální podpis je pojem ***elektronického podpisu***. Tento pojem v sobě zahrnuje (kromě samotného digitálního podpisu) také aspekty využití celé škály různých biometrických metod. Je pak obvykle precizován tak, aby byl tzv. technologicky nezávislý. Je proto také vhodný pro použití v různých legislativních dokumentech. Zejména v průběhu posledních let se (z hlediska právních a technologických aspektů) dospělo k poznání nezbytnosti používat takto obecný pojem.
Biometrické metody, které jsou dnes používány, lze rozdělit do dvou základních typů:

a) *fyziologicky* založené techniky, které měří nějakou fyziologickou charakteristiku dané osoby. Sem patří např.: otisky prstů, charakteristiky duhovky, obličej, geometrie cév, charakteristiky uší, vůně, analýza obrazců DNA, charakteristiky potu atd.;

b) *behaviorálně* založené techniky, které se zabývají měřením chování příslušné osoby. Toto zahrnuje např.: verifikaci ručně psaných podpisů – dynamika podpisu, charakterizace úderů do klávesnice, analýza řečového projevu atd.

Zaznamenaná biometrická charakteristika může být různými cestami uložena na záznamové médium a později využita k identifikaci (autentizaci) příslušného jedince. Spolehlivost použitého systému pak spočívá v tom, jakým způsobem je daný systém autentizace chráněn proti celé řadě postupů, metod a technik útoků, které mohou být prováděny s cílem zneužít tuto autentizační metodu. Zatím nelze konstatovat vysoký stupeň rozšíření těchto technologií, mezi nejčastější patří využívání otisků prstů.

Digitální podpisy tak dnes zůstávají z hlediska praktického užití základní a nejvíce používanou variantou elektronického podpisu. Obecně se dá říci, že elektronické (digitální) podpisy jsou nejčastěji používány:

- pro vazby typu smluv v otevřených sítích (např. elektronický obchod, finanční transakce);
- v uzavřených systémech (Intranety);
- pro osobní účely;
- pouze pro identifikační a autorizační účely (oprávnění přístupu do výpočetního systému, identifikace webovského serveru,…);

- pro oficiální komunikaci s veřejnými institucemi (daňová přiznání, přenos dokumentů s právními důsledky,…) –tato oblast je zatím především perspektivní (a to vysoce), i když již dnes existuje celá řada konkrétních případů, kde jsou elektronické podpisy takto využívány.

Direktiva EU

Historie elektronických podpisů z hlediska legislativních aspektů není ve světě příliš dlouhá. V podstatě se jedná o období posledních pěti, možná spíše tří let. V roce 1995 byl přijat vůbec první dokument tohoto typu – UTAH Digital Signature Act. V Evropě ze zákonodárství jednotlivých zemí nutno uvést zejména německý zákon o digitálním podpisu z roku 1997. Velká Británie pracuje na příslušném zákonodárství již několik let, z evropských zemí stojí za zmínku i Itálie. Již brzy se však ukázalo, že v této oblasti (možná více než v jiných) je třeba, aby zákony v jednotlivých zemích provázel určitý jednotící prvek. Podepsané dokumenty snadno překračují hranice a je zapotřebí zachovat i pro tyto situace platnost příslušných elektronických podpisů, a to jak z hlediska jejich vytváření tak i ověřování. Důležitou iniciativou v tomto směru byl Modelový zákon UNCITRAL pro elektronický obchod (1997). V tomto dokumentu se poprvé objevila snaha vytvořit takový obecný přístup k elektronickým podpisům, který by byl nezávislý na konkrétních použitých technologiích.

Vývoj v této problematice však jde velmi rychle dopředu - např. přístup ve zmíněném dokumentu Uncitral je dnes již považován svým způsobem za zastaralý. Je to dáno tím, že v současnosti není provázen cílenou snahou vytvořit jednotnou smysluplnou koncepci, ale spíše slouží ke shrnutí toho podstatného, co se dnes ve světě v této problematice děje. Státy Evropské Unie pochopily nezbytnost jednotného přístupu k řešení elektronického podpisu (zejména v návaznosti na elektronický obchod na společném trhu). Objevily se první varianty Direktivy EU k elektronickému podpisu. Zhruba dva roky byly velice pečlivě diskutovány její principy, zaměření a konkrétní pojmy v ní obsažené. Konečně 30. 11. 1999 byla Direktiva EU k elektronickému podpisu schválena Evropskou komisí. Vlády jednotlivých členských zemí EU mají za úkol uvést tuto Direktivu do svého zákonodárství do poloviny roku 2001.

Sama Direktiva se zabývá elektronickými podpisy používanými pro autentizační účely jak z hlediska obecného přístupu, tak i z hlediska speciálního typu tzv. zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým ručně psaným podpisům. Jejím cílem tedy není pokrýt všechny oblasti, ve kterých se používá autentizace, ale zaměřuje se na právní platnost elektronického podpisu, který je připojen k elektronickému dokumentu. Direktiva rovněž stanoví požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy a další požadavky vztahující se k podepisující a ověřující straně. Tyto požadavky nutně vyžadují podporu v detailních normách a veřejných specifikacích, které rovněž splní požadavky evropských obchodních organizací.

Direktiva byla vypracována tak, aby byly dodrženy tři následující principy:

a) technologická neutralita (i když základním smyslem je orientace na technologie digitálních podpisů, je cílem direktivy zůstat neutrální a vyhovět tak i jiným technologickým principům);
b) pro poskytovatele certifikačních služeb není apriori definováno žádné schéma pro autorizaci k provádění těchto služeb tak, aby v budoucnu zde existovala principiální možnost technologických inovací;
c) rozpoznání zákonné platnosti elektronických podpisů tak, aby nemohla být popřena jejich platnost na základě toho, že jsou v elektronické podobě a byla zaručena ekvivalence s ručně napsaným podpisem.

V současné době představuje Direktiva velice progresivní a zároveň rozpracované řešení (z hlediska obdobných legislativních iniciativ ve světě).

Některé důležité pojmy v Direktivě

K přiblížení si vlastního pojetí Direktivy uveďme a stručně rozeberme některé základní pojmy v ní uvedené.

Elektronický podpis - jsou jím míněna data v elektronickém tvaru, která jsou připojena či logicky asociována k jiným elektronickým datům a která slouží jako metoda autentizace.

Zaručený elektronický podpis- tím je míněn elektronický podpis splňující následující požadavky:

(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.

Zkusme se nejprve podívat na tyto dva pojmy. Proč jsou vůbec zavedeny a k čemu jsou všechny ty podmínky u druhého z nich? Odpověď je třeba hledat v praxi. V řadě situací je samozřejmě nezbytné, aby elektronické podpisy měly všechny potřebné atributy, tj. autentizaci autora, neporušitelnost zprávy, atd.
Pak je samozřejmě používána ta druhá, náročnější, definice zaručeného elektronického podpisu. Existují však praktické situace, kdy vystačíme s podstatně nižšími požadavky. Například u standardní e-mailové zprávy se spokojíme s vytištěným podpisem odesílající strany, neověřujeme obvykle telefonní číslo a adresu zásilkové služby, atd.

Pokud ovšem je nezbytné, aby ověřující strana měla určité záruky vzhledem k podepisující straně a vzhledem k obsahu podepsaného dokumentu, pak je třeba vytvořit takový rámec, v němž toto vše funguje. Specifikací tohoto rámce se zabývají podmínky (a)-(d).

Jaký smysl má např. podmínka (c) ? Co znamená ono slůvko „může“? Podívejme se na praktickou situaci s digitálními certifikáty veřejných klíčů, s certifikační autoritou a podepisovacím klíčem certifikační autority. Tady je třeba si uvědomit, že výše uvedená definice popisuje souhrnně jak vlastnosti elektronických (digitálních) podpisů jednotlivých uživatelů, tak i vlastnosti podpisu certifikační autority.

Popišme za tímto účelem, jak je prováděno podepisování certifikátů podepisovacím klíčem certifikačních autorit. Existují k tomu příslušná speciálně vyráběná hardwarová zařízení, kde je uložen soukromý (podepisovací) klíč CA. Tento klíč je zde uložen v zašifrovaném tvaru, je zašifrován jiným klíčem (označme ho např. EncKey). Podepisovací klíč nikdy toto zařízení neopustí v nešifrovaném tvaru. Vlastní akt podpisu pomocí podpisového klíče CA probíhá přímo v tomto speciálním zařízení (což může být např. čipová karta s příslušným firmwarem). Aby však toto podepisování mohlo být spuštěno, je třeba mít k dispozici klíč EncKey. Tento klíč je vytvářen opět přímo v tomto zařízení a sice pomocí tzv. sdíleného tajemství. To znamená, že se sejde (např.) minimálně šest z deseti oprávněných administrátorů. Každý z nich má na své kartě (kterou uchovává dle příslušných bezpečnostních směrnic) část onoho tajemství. Vložením potřebného počtu karet do zařízení je sdílené tajemství rekonstruováno, tj. je k dispozici EncKey. Pomocí tohoto klíče je pak dešifrován zašifrovaný podepisovací klíč CA.

Kdo je v této situaci podepisující osobou? Dle Direktivy EU je jí jednoznačně majitel (držitel) podepisovacího prostředku. A nyní se ukazuje i proč v onom bodu (c) je použito slůvko může. Vidíme, že majitel podepisovacího prostředku (obvykle tedy i majitel CA) si teoreticky může stáhnout jednotlivé karty s částmi tajemství a mít tak proces podepisování pod plnou kontrolou. Ovšem, z bezpečnostního hlediska, proč by toto dělal? Pro získání potřebného klíče, jak učí kryptografická praxe, je často nejjednodušší cestou jeho krádež. Pokud vlastník podpisového prostředku CA bude mít vše potřebné na jednom místě, stačí zloději provést pouze jedinou krádež. Ovšem v situaci, kdy k ochraně je použito sdílené tajemství, musí zloděj ukrást více jeho součástí (v našem případě tedy šest z deseti možných). A to bude určitě pro zloděje obtížnější.

Obraťme se k jiné dvojici pojmů, které Direktiva zavádí.

Certifikát **-** elektronické ověření, které propojuje data pro ověření podpisu s osobou a potvrzuje identitu této osoby.

Kvalifikovaný certifikát **-** certifikát, který splňuje podmínky uvedené v příloze I a je vydán poskytovatelem certifikačních služeb splňujícím podmínky uvedené v příloze II.

Příloha I přitom specifikuje, co vše musí kvalifikovaný certifikát obsahovat (identifikace poskytovatele certifikačních služeb, jméno či pseudonym podepsané osoby, pro jaké účely byl certifikát vydán, data pro ověření podpisu, počátek a konec doby platnosti certifikátu, zaručený elektronický podpis příslušného poskytovatele certifikačních služeb, omezení účinnosti certifikátu, atd).

Příloha II. stanoví povinnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty. Např. prokázání dostatečné spolehlivosti, zabezpečení příslušných operací v bezpečném adresáři, okamžitou službu pro revokaci certifikátů, zajištění správnosti časové identifikace pro vydání a odvolání certifikátu a zajištění množství dalších víceméně bezpečnostních opatření, nutných pro bezchybnou funkčnost certifikační služby.

První pojem - certifikát - opět slouží pro obecnou orientaci a běžné transakce bez velkých nároků. Naopak kvalifikovaný certifikát slouží jako nástroj určitého stupně důvěry a je určen pro použití v záležitostech s určitými bezpečnostními nároky. V praxi jednotlivé CA zatím řeší otázku důvěryhodnosti certifikátů jejich roztříděním do několika tříd (obvykle čtyř až pěti). Přitom např. certifikáty třídy nula neposkytují žádné bezpečnostní garance, majitel certifikátu se nemusí prokazovat obvykle žádnými doklady, výchozím údajem je třeba e-mailová adresa. Takovéto certifikáty jsou většinou vytvářeny pro demonstrační cíle. Naopak u certifikátů nejvyšších tříd kladou CA vysoké nároky na osobní prověrku dokladů majitelů budoucích certifikátů, prověrku příslušných oprávnění, atd. Tyto certifikáty samozřejmě již plně snesou označení kvalifikovaný certifikát.

Direktiva dále precizuje přesný obsah celé řady dalších souvisejících pojmů: podepisující osoba, data pro vytváření podpisu, data pro ověřování podpisu, prostředek pro vytváření podpisu, atd.

Klíčové momenty Direktivy

Možná že při prvním seznámení se s Direktivou nám zůstanou za přehršlí různých pojmů skryty některé základní ideje tohoto dokumentu. Zkusíme se proto na ni podívat i z jiných úhlů.

Především z hlediska praktických důsledků je velice významná následující formulace: „Členské státy nesmí přijmout předpisy stanovující, že provádění certifikačních služeb bude předmětem schvalovacího řízení.“ Toto v praxi znamená, že činnost certifikačních autorit obecně nepodléhá nějakému schvalovacímu řízení. Obecně řečeno, principy Direktivy jsou v řadě ohledů velice liberální. Cílem Direktivy je mj. umožnit neomezený pohyb odpovídajících technologií v rámci celého evropského trhu.

Dle terminologie Direktivy lze usoudit, že do praktického života budou zasahovat tři základní typy certifikačních autorit (v terminologii Direktivy – poskytovatelů certifikačních služeb). Kromě nejnižšího stupně, jehož činnost není Direktivou (zákonem) nijak upravována, to budou certifikační autority vydávající kvalifikované certifikáty (to bude stupeň, který bude běžný zejména v komerční sféře) a konečně akreditované certifikační autority. Certifikační autority vydávající kvalifikované certifikáty budou podléhat státnímu dohledu, stát je však může postihnout nejvýše finančními sankcemi, nemůže jim např. zastavit činnost. Stát však může v případě akreditovaných CA akreditaci (která je dobrovolná) odebrat.

Direktiva také vytváří bohatou strukturu i z hlediska samotných podpisů. Kromě již zmíněných pojmů, elektronický podpis a zaručený elektronický podpis, hraje důležitou roli (zejména z právního hlediska) i následující pojem. Je to elektronický podpis, který je za prvé zaručený, za druhé založen na kvalifikovaném certifikátu a za třetí byl vytvořen pomocí prostředku pro tzv. bezpečné vytváření podpisů. Poslední pojem „bezpečného“ prostředku je rovněž termínem Direktivy a svým způsobem označuje prostředek, který prošel „validací“, tj. bylo prokázáno, že jeho technologická konstrukce byla provedena tak, aby prostředek splnil celou řadu obsahových i bezpečnostních norem. Elektronický podpis, který má všechny tři výše zmíněné atributy (v dokumentech navazujících na Direktivu se tomuto podpisu říká **kvalifikovaný elektronický podpis**), má potom z hlediska práva příslušnou vypovídací schopnost. Přesněji dle formulace Direktivy- bude splňovat právní požadavky na podpis ve vztahu k údajům v elektronické podobě ve stejné míře, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k údajům psaným na papíře; a bude přijímán jako důkaz v soudním řízení.

Komplexní přístup k řešení – zpráva EESSI (European Electronic Signature Standardisation Initiative)

Kromě vlastní Direktivy je pro řešení problémů souvisejících s praktickými aplikacemi elektronických podpisů v zemích EU velice důležitým dokumentem závěrečná zpráva EESSI (červenec 1999, Final Report of the EESSI Expert Team).

Základním cílem dokumentu je analýza budoucích potřeb v oblasti standardizace na podporu Evropské Direktivy pro elektronický podpis. Odborná komise (zástupci průmyslových odborníků z jednotlivých členských zemí EU) zpracovala rozsáhlý a odborně fundovaný zásadní dokument [1], který spatřil světlo světa v červenci 1999. Jeho cílem nebylo ustavení povinných standardů a norem, které by podporovaly Direktivu, ale spíše identifikace požadavků, které by měly pomoci otevřenému trhu produktů a služeb splňujícím požadavky Direktivy.

Nejdůležitější závěry dokumentu:

1) převzetí resp. vývoj průmyslových norem by mělo maximálně zmenšit potřebu detailizace zákonů a vyhlášek v dané oblasti;
2) normy jsou nezbytně nutné a všude, kde je to možné, je třeba preferovat odkazy na existující mezinárodní normy před vývojem nových norem;
3) požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů;
4) podepisovací prostředky (produkty), pokud vyhovují požadavkům Direktivy, musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí pod EN 45000 (Evropské akreditační schéma);
5) je třeba vytvořit společný referenční bod na základě definice výchozí množiny technologických komponent, který bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty;
6) vzhledem k poskytovatelům certifikačních služeb je třeba použít vhodné bezpečnostní normy:
   - obecné zásady v oblasti bezpečnosti (např. BS7799 č. 1 a č. 2),

- specifikace bezpečnostních požadavků vzhledem k důvěryhodným systémům, které tito poskytovatelé používají; první požadavky v této oblasti se týkají především kryptografických modulů (např. FIPS 140-1) a využití rizikové analýzy,
- výchozí certifikační politika pro poskytovatele certifikačních služeb – je doporučováno vyjít z materiálu IETF PKIX – rfc. 2527,
- obdobně pro poskytovatele služeb v oblasti časových razítek je třeba provést specifikaci požadavků vzhledem k jejich politice;

7) vzhledem k produktům sloužícím k vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:
   - specifikace bezpečnostních požadavků vzhledem k důvěryhodným hardwarovým zařízením, která jsou použita jako bezpečná zařízení pro vytváření podpisů (FIPS 140-1, Common Criteria – ISO 15408),
   - specifikace pro vytváření elektronických podpisů (včetně uživatelova interface) a specifikace produktů a postupů k ověřování podpisů;
8) je nezbytná koordinace jednotlivých aktivit v oblasti norem;
9) z hlediska interoperability jsou nezbytné následující normy:
   - technické normy pro syntaxi a kódování elektronických podpisů (včetně vícenásobných podpisů); je doporučováno vyjít z rfc.2315,
   - operativní protokoly pro řízení PKI (rfc skupiny PKIX),
   - profily kvalifikovaných certifikátů na bázi X.509.

Samotný dokument obsahuje velice užitečné analýzy jednotlivých okruhů problémů a může sloužit jako kvalitní východisko i pro řešení řady praktických problémů v oblasti elektronických podpisů, certifikátů a poskytovatelů certifikačních služeb. Tým expertů EESSI v současnosti ve své práci pokračuje.

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 tomto článku, činnosti poskytovatelů certifikačních služeb. Podrobněji se lze s přehledem existujících norem seznámit ve zmíněném dokumentu EESSI nebo v [1].

Národní akreditační schéma

Direktiva předpokládá, že v každé členské zemi bude ustaveno vlastní akreditační schéma pro poskytovatele certifikačních služeb. Toto schéma bude založeno na principu dobrovolnosti (není tedy nutné, aby mu vyhověl každý poskytovatel certifikačních služeb) a bude sloužit vlastně jako určité rozšíření služeb poskytovatelů směrem ke zvýšení důvěryhodnosti, bezpečnosti a kvalitě. Toto akreditační schéma musí být objektivní, transparentní, úměrné a nediskriminující. Dle ustavení Direktivy musí být např. kvalifikované certifikáty vydané poskytovateli certifikačních služeb, kteří jsou akreditováni dle národního akreditačního schématu jedné členské země, právně uznávané v ostatních členských zemích EU.

Členské země EU jsou dle Direktivy povinny poskytovat následující informace (komisi EU a ostatním členským zemím):

a) o národním akreditačním schématu;
b) jména a adresy národních institucí zodpovědných za akreditaci a dohled;
c) jména a adresy všech poskytovatelů certifikačních služeb.

Jak je na tom Česká republika?

V České republice jsou otázky související s přípravou národního zákona o elektronickém podpisu v pozornosti odborné veřejnosti již delší dobu – zhruba dva roky. Prvním iniciátorem těchto snah byl ÚSIS (Úřad pro státní informační systém).

V loňském roce přišel s význačnou iniciativou v tomto směru SPIS (Sdružení pro informační společnost). Na základě jeho podnětu připravil doc. Smejkal postupně několik verzí tohoto zákona. Jedna z těchto verzí byla jako poslanecký návrh předložena parlamentu.

Ihned poté, co se odborná veřejnost s tímto návrhem seznámila, vznikla celá série závažných připomínek kritizujících zejména následující dva momenty. Smejkalův návrh vycházel především z pojetí

UNCITRAL, což z hlediska praktické užitečnosti zákona není příliš šťastné. Pojetí Direktivy je v každém směru výrazně dál a zejména - podporuje existující praxi. Druhým kritickým momentem návrhu byla existence velikého množství konkrétních chyb (převážně odborného charakteru) při jednotlivých formulacích. Vzhledem k vzniklé nezbytnosti přepracovat návrh zákona na příslušné odborné úrovni byla v únoru 2000 ustavena odborná komise (pod ÚSIS) , která si vzala za úkol zpracovat novou verzi zákona o elektronickém podpisu. Na práci komise se postupně v jednotlivých etapách podílela celá řada významných českých odborníků pro oblast elektronických podpisů. Význačným momentem práce komise bylo její pracovní zasedání v Třešti ve dnech 26. a 27. února 2000. Zde se podařilo dospět k jednotnému názoru na budoucí podobu zákona, a to jak z hlediska odborné komise tak i ÚSIS a SPIS. Jeden nedostatek je však třeba uvedenému postupu přiznat. Na zpracování tak důležitého zákona (pro celou oblast IT), bylo nakonec toho reálného času velmi málo.

Vzniklý návrh je koncipován na základě východisek Direktivy Evropské Unie a formulován tak, aby zabezpečil plnou kompatibilitu s požadavky v ní obsažených.

Tento přístup má dvě základní výhody:

1) zabezpečí v požadované míře naše přiblížení k zákonům EU;
2) umožní vytvořit národní zákon o elektronickém podpisu na bázi v současné době nejprogresivnější světové platformy pro tuto problematiku.

Ing. Jaroslav Pinkava, CSc.
jaroslav.pinkava@aec.cz

Ing. Jaroslav Pinkava, CSc.
Jaroslav Pinkava, nar. 2.5.1948, kandidát matematicko-fyzikálních věd. Začínal na katedře statistiky VŠE v Praze, od roku 1978 se věnuje profesionálně kryptologii. V současné době pracuje jako kryptolog brněnské firmy AEC spol. s r.o.. Je místopředsedou kryptologické skupiny JČMF, členem IACR. V roce 1999 byl členem organizačního výboru mezinárodní konference Eurocrypt´99 (Praha - květen).

MS

Využívání digitálních podpisů pro oblast IT je již řadu let v popředí zájmu. Kromě vlastních technologických principů je nezbytné zabývat se celou řadou navazujících otázek. Nejdůležitější z nich jsou legislativní a standardizační aspekty problematiky. V této souvislosti se článek zabývá situací v Evropské Unii, popisuje nejdůležitější dokumenty, jako jsou Direktiva EU k elektronickým podpisům a závěrečná zpráva skupiny expertů (Final report EESSI – July 1999). V České republice chystaný zákon o elektronickém podpisu by měl být plně kompatibilní s požadavky EU a svým obsahem a kvalitou by měl napomoci praktickému využívání těchto moderních technologií.