ZÁKON O ELEKTRONICKÉM PODPISU

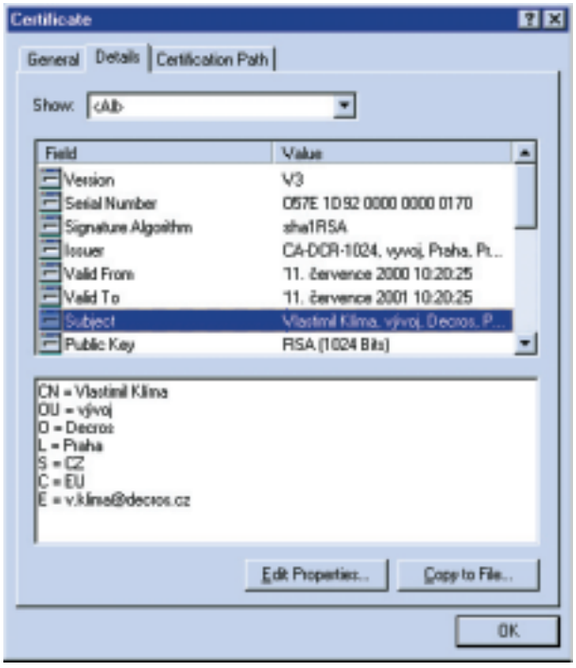
Expres neujel, otázky zůstávají

Česká republika je první zemí ve střední a východní Evropě, kde byl po vydání příslušné směrnice EU schválen zákon o elektronickém podpisu. Zákon nabývá účinnosti již 1. 10. 2000 a samozřejmě nás zajímá, jak bude působit v praxi. Popsali jsme proto, jak by mohl fungovat, a – neboť řeč paragrafů není právě nejsrozumitelnější – také jsme položili spoustu otázek spolutvůrci zákona.

ZÁKON O ELEKTRONICKÉM PODPISU PLATÍ

Loni jsme vás v čísle 11 poprvé informovali o návrhu zákona v článku „Stihneme informační expres?" (viz infotipy). Vysvětlili jsme zde základní pojmy návrhu zákona i asymetrické kryptografie – bez jediného vzorce, a tedy pro nejširší veřejnost (k pojmům se můžete vrátit, nebudeme je zde opakovat). Od té doby text zákona doznal značných změn, ale podstatné je, že nyní už platí – je to **zákon č. 227/2000 Sb.** (dále jen ZoEP). Můžeme tedy přemýšlet, jak ho využít v praxi a co umožňuje. A pokud něco neumožňuje, usilovat o novelizaci v tomto směru.

Při čtení zákona nás napadla řada otázek, na něž jsme si jako laici z právního hlediska nedokázali odpovědět. Zeptali jsme se proto spolutvůrce zákona, doc. ing. Vladimíra Smejkala, CSc. (pravidelní čtenáři Chipu ho dobře znají jako kmenového autora právní rubriky). Také vám doporučujeme si zákon nejprve přečíst a pak se podívat na otázky a odpovědi – vše najdete na vloženém Chip CD (viz infotipy). Doufáme, že to bude dostatečný impulz, abyste se sami začali ptát, co a jak lze využít a jestli zákon pomáhá nebo brání vašim záměrům v této oblasti. Budeme rádi, pokud nám své postřehy nebo otázky pošlete. Chtěli bychom rozvinout diskusi, jak zákon „zprovoznit" v elektronickém obchodu, v kontaktech občana se státem, v bankovnictví a v co nejvíce dalších oblastech.



Typický certifikát zaměstnance vydaný firemní certifikační autoritou

DIGITÁLNÍ, NEBO ELEKTRONICKÝ PODPIS?

Ještě před vydáním směrnice EU o elektronickém podpisu měl náš zákon hovořit o digitálním podpisu (DP), který je založen na kryptografii s veřejným klíčem. Po vydání směrnice byly zavedeny obecnější pojmy – *elektronický podpis* (EP) a *zaručený elektronický podpis* (ZEP) jako jeho silnější verze. Je možné, že se tímto krokem kuriózně zlegalizovala i možnost EP bez asymetrické kryptografie, to ale nelze bez odborného výkladu zákona zjistit, a dokonce se zdá, že to budou muset vyjasnit až prováděcí předpisy.

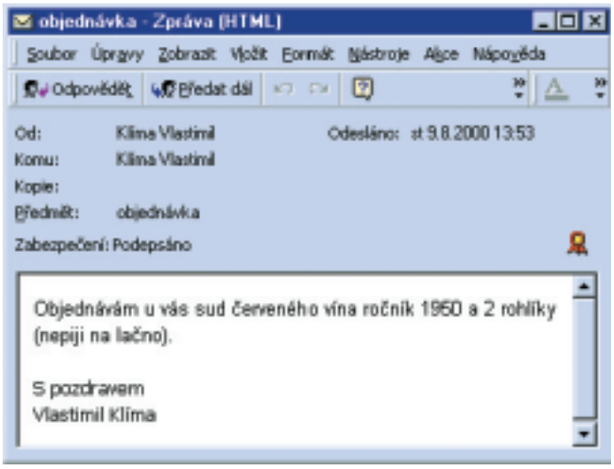
JAK TO FUNGUJE

Digitální podpisy jsou v počítačovém světě běžně spojovány výhradně s asymetrickou kryptografií a jsou reálně používány i bez právní základny (typu ZoEP) řadu let (bezpečný přístup na web, spouštění programů z internetu apod.). Nyní si tento model přeneseme k nám a podíváme se, jak by mohl fungovat pro našeho občana.

Tak tedy: pan Novák si určitým programem doma, v informačním kiosku nebo na pracovišti certifikační autority vygeneruje asymetrický pár klíčů, z nichž jeden je *veřejný* a druhý *privátní*. Privátní klíč udržuje v tajnosti a chrání si ho, protože ho bude používat k vytváření digitálního podpisu. Klíč bude mít obvykle uložený na disketě, v počítači nebo v čipové kartě a jeho použití bude většinou ještě jištěno nějakou formou PIN (podobně jako u bankovní karty).

Je v zájmu pana Nováka, aby jeho veřejný klíč byl dostupný komukoliv. Bude totiž sloužit jeho partnerům (ostatním občanům, obchodníkům a organizacím) k ověřování jeho podpisu. Novák teď bude totiž chtít svým klíčem digitálně podepisovat kdeco – bankovní příkazy, daňová přiznání atd. K tomu je ale potřeba, aby jeho veřejný klíč byl nejen k dispozici všem, kdo mají platnost jeho digitálního podpisu ověřovat (obchodníci, státní správa, občan), ale aby také měli jistotu, komu tento klíč ve skutečnosti patří. Z tohoto důvodu se zavádějí *certifikáty* a *certifikační autority* (CA), kterým zákon říká *poskytovatelé certifikačních služeb*.

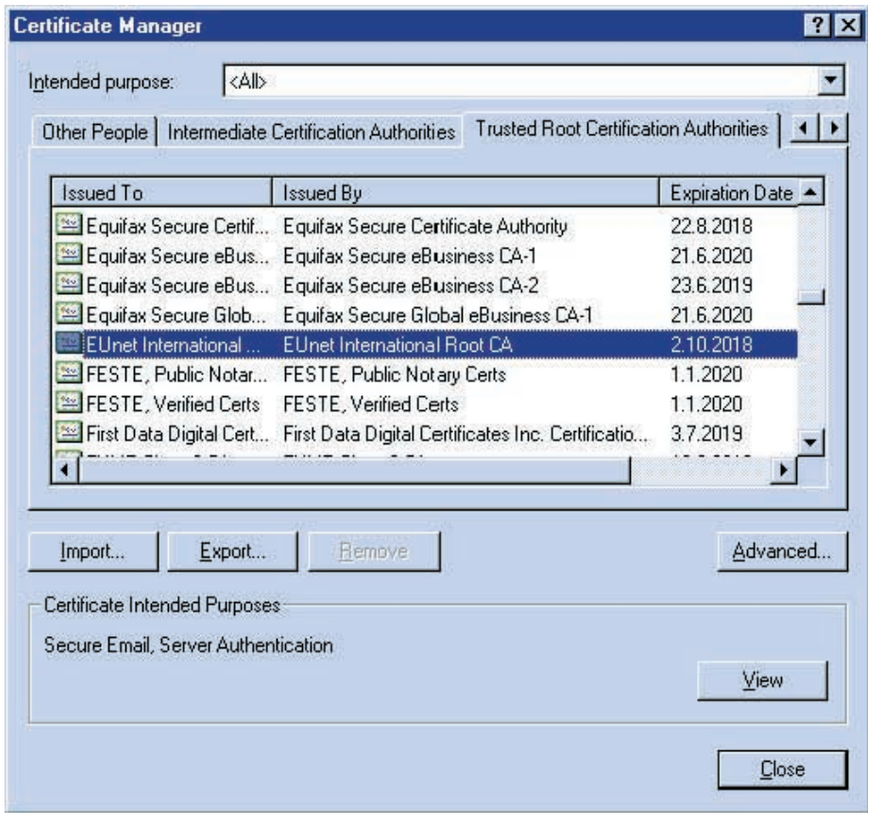
CA je tu zjednodušeně řečeno proto, aby stvrdila propojení občana s jeho veřejným klíčem. Proto v certifikátu, který CA Novákovi vydá, musí být Novákův veřejný klíč a nějaké jeho vhodné „identifikační znaky". Navíc může obsahovat jakékoliv další údaje, o nichž ještě bude řeč. V praxi budou certifikáty vydávány asi za poplatek, neboť CA podle našeho zákona bude mít odpovědnost za to, že údaje v certifikátu o panu Novákovi ověřila (a tedy že jsou platné), ale nemusí tomu tak být vždy. Za těchto předpokladů už základní model může začít fungovat.



Ikonka v záhlaví přijaté objednávky signalizuje, že zpráva byla digitálně podepsána. Pokud na ni klepneme (viz následující obrázek), získáme další informace o podpisu.

Co udělá občan

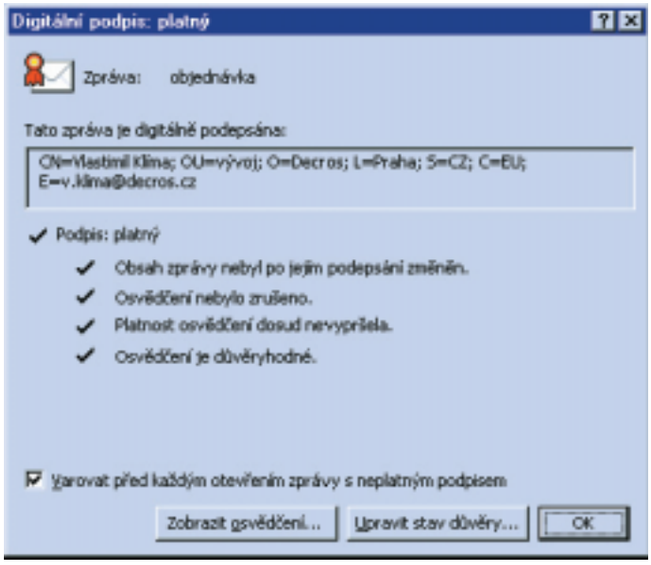
Chce-li pan Novák používat ZEP, bude postupovat (opět zjednodušeně) asi takto: Dostaví se k vybrané CA s osobními doklady, zde s ní sepíše smlouvu o vystavení certifikátu a na místě si na pracovišti CA (na zabezpečeném počítači) vygeneruje dvojici klíčů. (Může to ovšem také udělat doma pomocí programu od CA nebo obdobného programu veřejně dostupného.) Přitom také vyplní a právě vygenerovaným privátním klíčem rovnou digitálně podepíše také svoji tzv. žádost o certifikát (je to jeho první digitální podpis). V žádosti uvede identifikační údaje, které budou později vidět v jeho certifikátu – jméno a příjmení, může tam být i poštovní adresa, e-mail atd. Co všechno je v certifikátu uvedeno, záleží na jeho účelu a pravidlech CA a samozřejmě na ZoEP. Může tam být také nejvyšší částka, kterou může jeho držitel pomocí svého klíče a tohoto certifikátu elektronicky platit (je to pojistka certifikační autority proti případným škodám).



Seznam důvěryhodných kořenových CA, které uznává MS Internet Explorer 5.01.

Privátní klíč si (pokud ho už negeneroval doma) pak Novák odnese uložený na disketě, čipové kartě nebo jinak, podle toho, co mu CA poskytne. Veřejný klíč je naopak automaticky přidán do žádosti o certifikát. CA přijme žádost o certifikát, ověří Novákova identifikační data (jeho totožnost) a pomocí Novákova veřejného klíče na místě zkontroluje, zda jeho digitální podpis na žádosti je platný. Tím se mj. ujistí, že žadatel má odpovídající privátní podpisový klíč. Následně sama CA digitálně podepíše vyplněný formulář (certifikát), který kromě některých údajů od žadatele doplní ještě svými vlastními údaji o době platnosti certifikátu, své vlastní identitě, sériovém číslu certifikátu apod.

Takto podepsaný certifikát pak CA vhodným způsobem zveřejní (obvykle na svém webu) a obvykle ho také rovnou Novákovi nahraje na jeho médium. Od této chvíle mohou všichni, jimž pan Novák něco digitálně podepíše, ověřovat jeho digitální podpis.



Základní informace o podpisu zprávy z předchozího obrázku. Podpis je platný. Klepnutím na „Zobrazit osvědčení" získáme další informace o certifikátu a certifikační cestě.

Stačí jim k tomu stáhnout si Novákův certifikát, z něho přečíst jeho veřejný klíč a pomocí něj ověřit platnost jakéhokoliv konkrétního Novákova digitálního podpisu. Navíc v certifikátu jsou s tímto veřejným klíčem spojeny identifikační údaje o Novákovi. Jakou mají „právní sílu" a za co ručí certifikační autorita, o tom rozhoduje zákonodárství daného státu. A právě to také mj. řeší náš ZoEP.

Co udělá stát

Teď se podívejme na druhou stranu mince. Pan Novák (obchodní ředitel nějaké firmy) nám digitálně podepíše objednávku za milion korun. Abychom si ověřili jeho podpis, stáhneme si nejprve Novákův certifikát z webu jeho certifikační autority (dejme tomu, že se jmenuje BigCA) a také veřejný klíč BigCA. Tímto veřejným klíčem pak ověříme Novákův certifikát a všechno je, zdá se, v pořádku.

Jak ale ověříme, že BigCA není fiktivní a že ji Novák nenastrčil na internet? Tato hrozba je reálná a v počítačovém světě se odstraňuje tzv. certifikační cestou (a kořenovou certifikační autoritou) nebo křížovými certifikáty.

Oč tedy jde? Platnost veřejného klíče Novákovy certifikační autority BigCA můžeme ověřit certifikátem, přičemž CA ve světě fungují trojím způsobem: jako tzv. samocertifikující se (pseudokořenové) CA (certifikát si tato autorita vydala sama a sama si ho podepsala), kdy klíč takové CA pak ale musí být ověřitelný nějakým jiným důvěryhodným způsobem (Úřadem pro elektronický podpis, publikací ve Zlatých stránkách, na bezpečném webu státní instituce apod.). Druhou možností je, že veřejný klíč BigCA podepíše jiná certifikační autorita. Této „nadřízené" autoritě může certifikát podepsat jiná „nadřízená" autorita atd., čímž vzniká tzv. *certifikační cesta* (řetězec nebo strom), končící u nejvyšší autority, která se v tomto případě stává autoritou kořenovou. A opět u ní musí být možnost ověření jejího certifikátu jako u prosté kořenové autority, jak bylo popsáno výše.

Třetí možností je tzv. *křížový certifikát*, kdy si dvě certifikační autority podepíší své certifikáty vzájemně. Tím se stávají jedna nadřízená druhé, a tudíž rovnocenné. To je výhodné například u dvou firemních CA. Novák (zaměstnanec) zde věří své CA, a navíc prostřednictvím křížového certifikátu může věřit i certifikátům zaměstnanců druhé firmy (ještě lépe, pokud se tak firmy smluvně dohodnou).

U nás bude platnost veřejných klíčů certifikačních autorit potvrzovat dozorový Úřad pro ochranu osobních údajů, alespoň u těch CA, které se musí u něj ohlásit (vydávají-li kvalifikované certifikáty) nebo akreditovat (působí-li v oblasti veřejné správy). U ostatních CA zákon nepředepisuje nic, takže zde mohou křížové certifikáty a certifikační cesty fungovat. Uznávání zahraničních CA zákon řeší dvojím způsobem: zárukou tuzemské CA za certifikáty vydané zahraniční CA nebo schválením možnosti používání certifikátů konkrétní zahraniční CA Úřadem.

Terminologie

Jak jsme už předeslali, náš ZoEP zavádí obecnější terminologii pro právě uvedené pojmy z oblasti DP. Proto místo o DP, který je dnes spojován s asymetrickou kryptografií, hovoří o EP a ZEP. Také rozeznává dva druhy certifikátů, různé druhy certifikačních autorit (obyčejné, vydávající kvalifikované certifikáty, akreditované) a zavádí instituci, která vykonává dozor nad dodržováním tohoto zákona, uděluje akreditace a vydává prováděcí předpisy. O tom, do jaké míry a s jakými zárukami budou použitelné výše uvedené modely, které fungují v počítačovém světě, rozhodne výklad ZoEP. Ten bohužel není možné vyčíst z textu zákona bez pomoci právníka. Obáváme se také, že výklady různých právníků se mohou velmi lišit, protože se jedná o dost neobvyklý a vlastně „přelomový" zákon. Hodně z toho by také měly objasnit prováděcí předpisy. Jejich vydání bude klíčové a je očekáváno s velkým zájmem a netrpělivostí.

Závěr

Dovolte mi na závěr poděkovat doc. Smejkalovi za odpovědi na moje otázky, které naleznete na přiloženém Chip CD. Chci vás ještě jednou požádat o vaše další dotazy. Můžete je zasílat na moji adresu (v předmětu e-mailu prosím uveďte „FAQ-ZoEP-Chip") nebo do redakce. S odpověďmi vás brzo seznámíme a budeme vás také informovat o dalším dění na tomto poli.

Vlastimil Klíma, v.klima@decros.cz

infotipy

O podstatě elektronického podpisu bez vzorců:
Klíma, V.: Stihneme informační expres?, Chip 11/99, str. 52 – 53 a 56 – 58

Vize, jak digitální podpis může změnit náš život:
Klíma, V.: Až nás podepíše počítač, Chip 5/99, str. 36 – 39
(oba články jsou též na
www.decros.cz/Security_Division/Crypto_Research/archiv.htm)

O zákonu z právního hlediska:
Smejkal, V.: Proč nový zákon?, Chip 11/99, str. 54 – 55.
Smejkal, V.: Elektronický podpis se blíží,
www.znalci.cz/clanky/pdf/epodpis.pdf

Web iniciátora zákona:
www.spis.cz

Zákon 227/2000 Sb.:
Chip CD 10/00, Chip Plus – Infonet

Otázky a odpovědi k ZoEP:
Chip CD 10/00, Chip Plus

ZÁKON O ELEKTRONICKÉM PODPISU

Zatímco v textu kolegy Klímy se můžete dočíst o metodách a postupech při elektronickém podepisování, zde bych se rád stručně zmínil o **právních aspektech zákona č. 227/2000 Sb. o elektronickém podpisu** (ZoEP).

Zákon nevznikl sám od sebe a izolovaně v České republice. Je výsledkem několikaletého snažení a kvašení v mezinárodních organizacích, které se nejprve pokusily definovat nějaký univerzálně použitelný dokument, který by se vztahoval k momentálně nejpalčivějším otázkám, tj. elektronickému obchodu. Proto na půdě Komise OSN pro mezinárodní obchodní právo (United Nations Commission on International Trade Law – UNCITRAL) vznikl tzv. *Vzorový zákon o elektronickém obchodu.*[1] Jde o návrh velmi obecný, který má sloužit všem zemím, jež v souladu s technologickým pokrokem potřebují modernizovat svoji legislativu.

Charakteristickým rysem elektronického obchodu je, že zahrnuje datové zprávy a elektronické podpisy, což představuje podstatný rozdíl oproti tradičním dokumentům v tištěné formě. Vzorový zákon vychází z úvahy, že uživatelé budou potřebovat ucelený soubor pravidel použitelných na různé druhy komunikačních prostředků, které by bylo možné při jejich používání vzájemně zaměnit, a že zásadně žádný z komunikačních prostředků není z rozsahu navrhovaných řešení vyloučen, protože je nutno přihlédnout k budoucímu technickému vývoji. Vzorový zákon spočívá na tzv. „funkčně ekvivalentním přístupu", vycházejícím z analýzy účelů a funkcí vyžadovaných od tradičních, na papíře vytištěných dokumentů, s ohledem na to, do jaké míry lze tyto účely či funkce realizovat elektronicko-komerčními prostředky.

„Klasický" dokument na papíře poskytuje určité užitné hodnoty, mezi něž mj. patří: jistota, že každý si může dokument přečíst; možnost zajistit, aby dokument nepodléhal změnám v čase; možnost takové jeho reprodukce, aby každá ze stran mohla vlastnit kopii se stejnými údaji; možnost ověření údajů podpisem; možnost existence dokumentu v takové formě, kterou lze předložit úřadům a soudním dvorům. Datovou zprávu samu o sobě nelze považovat za naprostý ekvivalent dokumentu vytištěného na papíře pouze z toho důvodu, že její povaha je rozdílná a nutně nesplňuje veškeré možné funkce jako papírový dokument.

Je však třeba zdůraznit, že i při všech uvedených funkcích papíru může elektronický záznam poskytnout stejnou úroveň jistoty jako papír a (ve většině případů) podstatně vyšší úroveň spolehlivosti a rychlosti, zejména s ohledem na identifikaci zdroje dat – za předpokladu, že bude splněna řada technických a právních požadavků. Přijetí funkčně ekvivalentního přístupu by přitom podle vzorového zákona nemělo vyústit u elektronického obchodu v uložení přísnějších požadavků na bezpečnost (a s tím i spojených nákladů), než je tomu u dokumentů na papíře. Klíčová myšlenka zákona, že **informaci nelze upřít právní důsledky, platnost nebo vykonatelnost jen proto, že má formu datové zprávy**, je jistým převratem v doposud omezeném chápání písemností a dokumentace jakožto informací výlučně spjatých s papírovým nosičem.

Proč zatím nebyl tento návrh aplikován do právních řádů členských zemí OSN, má zřejmě více důvodů, mezi nimiž nepochybně figurují:

- obecnost, která je výsledkem mnoha kompromisů typických pro dokumenty OSN;
- z toho vyplývající obtížná aplikovatelnost;
- snaha většiny států nezavádět zvláštní právní úpravy tam, kde postačí stávající norma nebo její novelizace.

Evropské společenství, přestože členské státy mají daleko homogennější právní systémy než členové OSN, se vydalo cestou opačnou: vydáním směrnice, která stanoví „pravidla hry" pro jeden z nejdůležitějších aspektů elektronické komunikace, tj. elektronický podpis – s tím, že budou následovat další kroky upravující v rámci stávajícího právního rámce např. otázku odpovědnosti za škodu, obchodování na dálku, cel a daní, dálkového zaměstnání apod. To je asi vhodnější cesta, což potvrzuje i skutečnost, že práce na normě pro elektronický podpis přes počáteční pomalý rozjezd rychle finišovaly a dne 13. prosince 1999 spatřila světla světa závazná *Směrnice EU č. 1999/93/EC o zásadách Společenství pro elektronické podpisy.*

I tato směrnice je dosti obecná a také obsahuje řadu kompromisů, z nichž některé budou dělat národním legislativcům i odborníkům na technologii elektronického podepisování vrásky na čele. Zejména proto, že neexistuje jiný, výkladový nebo technologický dokument EU, který by na Směrnici navazoval a „vysvětloval" ji. (Výstupy jiných organizací a sdružení, např. často citovaného EESSI, nejsou zcela kompatibilní se Směrnicí a bude chvíli trvat, než dojde k jejich sladění, pokud se tak vůbec stane.)

Směrnice i český zákon jsou zaměřeny na právní aspekty daleko více než na technologické řešení, což vedlo k jistému nepochopení ze strany potenciálních poskytovatelů certifikačních služeb i uživatelů. Stále se opakují námitky, že zákon neřeší to či ono. Je třeba si ale uvědomit, že zákony nejsou ani technickými normami, ani technologickými předpisy, ani programovacími manuály. Už tak silný ohled na technologie, který bohužel do zákona vnesla zmíněná směrnice EU, považuji za nešťastný a v budoucnosti omezující. (Podle mých informací je to způsobeno silným německým vlivem v pracovní skupině DG XV, protože Německo již dříve mělo a používalo svůj zákon o digitálním podpisu,[2] a tedy řada aspektů z původního řešení se objevila i v nové směrnici.)

Český ZoEP je prvním, ale pravděpodobně nejdůležitějším krokem, na který bude muset ještě navazovat nařízení vlády, jak mají orgány vykonávající veřejnou správu zavést v praxi elektronické podpisy, vydání prováděcích předpisů pro citovaný zákon, vybudování sítě poskytovatelů certifikačních služeb a jejich dobrovolná akreditace u Úřadu pro ochranu osobních údajů.

Zákon definuje pojmy, postupy a subjekty práva účastnící se na vytváření, používání a ověřování elektronických podpisů a zaručených elektronických podpisů jako prostředků umožňujících používání elektronických dokumentů (datových zpráv) způsobem, který je v souladu s obecně závaznými právními normami.

Zákon č. 227/2000 Sb. o elektronickém podpisu velmi nenápadně uskutečnil také **novelu** všech hlavních procesních právních norem: **občanského soudního řádu, správního řádu, trestního řádu a zákona o správě daní a poplatků**, v nichž byla zakotvena alternativní možnost elektronického podání opatřeného zaručeným elektronickým podpisem. Rovněž byla provedena novela § 40 **občanského zákoníku, upravujícího podepisování**.

Zákon, přes intenzivní odpor autorů návrhu zákona, respektuje totální liberalizaci vyplývající ze směrnice EU, i když se nám v našich podmínkách jeví tato liberalizace jako poněkud předčasná. Rozlišuje proto **dvě kategorie poskytovatelů** certifikačních služeb vydávajících

kvalifikované certifikáty: **akreditované** dozorovým orgánem (Úřadem pro ochranu osobních údajů) a **ostatní**. Není-li poskytovatel certifikačních služeb akreditován Úřadem, je alespoň povinen ohlásit Úřadu nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu, že bude vydávat kvalifikované certifikáty. To proto, aby mohl Úřad na systém kvalifikovaných certifikátů dostatečně dohlížet a sankcionovat porušování zákona (pokutami až do výše 20 000 000 Kč).

Požadavky kladené na poskytovatele jsou obsáhlé a u akreditovaných poskytovatelů zákon mj. stanoví, že musejí mít sídlo na území České republiky a pro výkon dalších činností mimo tyto služby mít souhlas Úřadu. Není vhodné, aby např. banka fungovala současně jako poskytovatel certifikačních služeb (PCS), protože potom by se z „trojúhelníku důvěry" – klient, banka, třetí strana ručící za propojení veřejného klíče s identifikovanou osobou – stala přímka mezi bankou a klientem.

Aby byla zaručena vysoká důvěryhodnost elektronického podání a elektronické komunikace ve veřejné správě, byl zcela v souladu se směrnicí EU začleněn do zákona požadavek, že **v oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty, vydávané akreditovanými poskytovateli certifikačních služeb**. (Ostatní, tzv. neakreditovaní poskytovatelé těchto služeb mohou fungovat také, ale pouze pro soukromoprávní subjekty.) Přísné podmínky pro fungování PCS vyplývají z obavy z možného zneužití systému elektronického podepisování, přičemž podle názoru autorů i navrhovatelů zákona není problémem po nějaké době, po získání zkušeností a (doufejme) po zvýšení etiky českého podnikatelského i občanského prostředí, učinit další liberalizační kroky.

V České republice nyní probíhají analytické práce na téma, jaká další legislativní opatření potřebujeme pro prosazení elektronického obchodu. Jelikož žádné výstupy nebyly oficiálně publikovány, nemůžeme odhadnout, zda je snahou vlády vytvořit zvláštní právní úpravu pro elektronický obchod, zda se bude postupovat cestou dílčích novel, nebo zda je analýza orientována spíše organizačně nebo technologicky. Mlčení a kusé informace okolo těchto prací jsou poněkud podivné. Osobně se domnívám, že nejsprávnější cestou je postupná novelizace právního řádu a revize všech stávajících norem z hlediska moderních informačních technologií.

Poté, co byly přijaty dva zásadní nové zákony (zákon č. 101/2000 Sb., o ochraně osobních údajů, a ZoEP), a až bude přijata novela občanského zákoníku upravující obchody na dálku, bude z hlediska české legislativy učiněn velký krok směrem k elektronickému obchodování. Ještě ale zůstanou k vyřešení další otázky, které už jsou diskutovány na mezinárodních fórech, zatím však bohužel ne u nás: **rozhodné právo na internetu, cla a daně u obchodu s nehmotnými statky, právní povaha jmen domén včetně případných změn v systému přidělování jmen domén v ČR** a další.

VLADIMÍR SMEJKAL, VSMEJKAL@COMP.CZ

[1] Viz Smejkal, V., Mates, P.: Internet – *Vzorový zákon UNCITRAL.* Právní rádce, VII., č. 11/1999, s. 16.
[2] Zákon o informačních a komunikačních službách (Informations- und Komunikationsdienstgesetz).