Návrh zákona o elektronickém podpisu

---

23. září byl zveřejněn návrh českého zákona o elektronickém podpisu. Jedná se o zatím nejpokrokovější zákon o elektronickém podpisu v Evropě, a pokud vše půjde ideálně, může být schválen do osmi měsíců. Abychom zákon pochopili, vysvětlíme si jeho technickou podstatu.

Stihneme informační expres?

Na úvod si řekněme několik informací o návrhu tohoto zákona (dále pro jednoduchost jen "zákon"), protože je výjimečný v několika směrech. Především jsou to okolnosti jeho vzniku a rychlost, jakou byl vypracován.

Autory zákona jsou docent Mates a docent Smejkal (posledně jmenovaného znáte ze stránek Chipu) a jeho předkladateli vládě budou čtyři poslanci, kteří jsou zároveň místopředsedy čtyř politických stran. S touto podporou je reálná šance, že Parlamentem a Senátem projde bez politických průtahů.

Vypracování zákona iniciovalo Sdružení pro informační společnost (SPIS), jehož členem je 39 významných firem z oblasti informačních a telekomunikačních technologií. Zákon byl společně s důvodovou zprávou předložen k diskusi široké veřejnosti na internetu (*www.spis.cz*). O připomínkách se hovořilo 4. 10. u kulatého stolu "Česká republika na cestě k informační společnosti" na Invexu a i o nich se dozvíte na uvedené adrese.

Jedná se o dosti "technický" zákon, jehož pochopení proto silně závisí na znalosti významu odborných termínů. Navíc právě proto, že jde v oblasti elektronických podpisů dále než obdobné zahraniční právní normy, je i jeho odborná terminologie bohatší. Tak například právě pojem "elektronický podpis" je širší než "digitální podpis".

Návrhu zákona by přitom měli porozumět i lidé, kteří s elektronickou komunikací nemají zkušenosti, nebo budoucí uživatelé, kteří si nejsou jisti, co to je digitální nebo elektronický podpis, nebo netuší, jaký to může mít význam. Tento článek je určen především jim.

Začněme tím hlavním, o čem zákon pojednává, tj. elektronickým podpisem. Zákon rozeznává (obyčejný) ***elektronický podpis (EP)*** a ***zaručený elektronický podpis (ZEP)***. Hlavním předmětem zákona je **zaručený** elektronický podpis – k němu se také vztahuje 99 % textu zákona. Je to elektronický podpis, který je, stručně řečeno, **věrohodný a právoplatný**, zatímco (pouhý) elektronický podpis takový být nemusí. Příkladem elektronického podpisu je například text "Josef Švejk" na konci elektronické pošty nebo elektronického bankovního příkazu. **Pokud se komunikující strany dohodnou**, může jim elektronický podpis dávat stejné záruky jako zaručený elektronický podpis. Pokud se takto **nedohodnou**, zákon považuje za právoplatný **jen zaručený elektronický podpis**.

V současné době známe jen jeden příklad ZEP a tím je *digitální podpis (DP)*. Je to kryptografická technika, používající pojmy jako *tajný klíč* a *veřejný klíč*, *certifikační autorita (CA)*, *certifikát*, k nimž se

ještě vrátíme. Zákon se ale – docela prozíravě – nechce vázat na jedinou technologii, a proto tyto pojmy, vztahující se ke konkrétní technologii, nepoužívá. Vždyť může přijít jiná technologie, která bude mít všechny požadované vlastnosti, a vůbec nebude založena na kryptografii!

Máme-li však zákon vysvětlit, musíme se přidržet této jediné dnes známé technologie ZEP. Neuděláme tím ale žádnou chybu, protože uzákonění digitálního podpisu nám v současné době přinese ono elektronické obchodování, uzavírání vztahů na dálku a mnoho dalších příjemných věcí, tj. všechno to, proč byl zákon o EP vypracován.

Digitální podpis

Především je nutno si uvědomit, že **digitální podpis nemá nic společného s pojmy jako zdigitalizovaný podpis nebo naskenovaný podpis**. Digitální podpis je totiž jen a jen **číslo**! Můžeme si je představit jak v desítkové, tak v dvojkové či jiné soustavě. Je to jedno, protože každý z těchto tvarů můžeme vzájemně jednoznačně převést na druhý. Pro další výklad však asi bude názornější si číslo představit jako posloupnost nul a jedniček (bitů); naopak posloupnost bitů pak můžeme přirozeně považovat za vyjádření čísla. Od "běžných" čísel se ale digitální podpis přece jen odlišuje. Zejména tím, že

a) to bývá velmi velké číslo (o délce např. 1024 bitů),

b) jeho výpočet nebo ověření je dosti složitý úkon, který nelze provádět ručně, ale pouze pomocí počítače.

O tom, jak se toto číslo vypočítá, si řekneme později. Počítač, který umí vytvářet nebo ověřovat DP, nemusí být zrovna stolní počítač. Příslušně složité výpočty mohou vykonávat i miniaturní čipy, které se vejdou na čipové karty (ty se už delší dobu vyrábějí). V budoucnu mohou být takové čipy umístěny i v různých technických zařízeních, třeba v mobilních telefonech, klíčích od auta nebo hodinkách – vše záleží jen na představivosti uživatelů, na trhu a na tom, kterým směrem se celá tato oblast pohne. Prozatím tedy zůstaňme u toho, že digitální podpis je velmi velké číslo, které je vytvářeno nebo ověřováno počítačem.

Digitální dokument

Také pojem *digitální dokument* by mohl být trochu zavádějící – možná evokuje představu pouhé digitální obdoby nějakého formálního dokumentu (listiny, formuláře apod.). My zde ale budeme pod pojmem digitální dokument uvažovat **libovolný soubor dat** tak, jak jej známe z počítačové terminologie. Digitální dokument je tedy libovolná posloupnost dat, nebo chcete-li, libovolná posloupnost bitů (v zákoně tomuto pojmu odpovídá termín "datová zpráva").

Hlavním smyslem zákona je **zrovnoprávnit** papírové dokumenty s dokumenty digitálními a rukou psané podpisy s podpisy digitálními (obecněji se ZEP). To první, převod současných papírových dokumentů do digitální podoby, je poměrně jednoduché a u většiny současných papírových dokumentů není obtížné si představit jejich digitální ekvivalent. V nejhorším případě si vše, co je dnes napsáno, namalováno nebo jinak ztvárněno na papíře, můžeme naskenovat a poté pracovat se souborem dat, který nám skener předá jako "digitální kopii" dokumentu. Mnohem častěji jsou však digitálními dokumenty soubory dat, které přímo vznikají na našem počítači nebo s kterými zde pracujeme (soubory

textové, obrazové, zvukové, ...). Digitálními dokumenty mohou být ale i počítačové programy, zvukové sekvence nebo jednotlivé položky v databázi atd.

Podstatné je, že ve všech uvedených případech jde jen a jen o **posloupnosti bitů**. A protože posloupnost bitů můžeme chápat jako číslo, také digitální dokument bude pro nás **číslo**. Většinou to bude opět velké číslo, třeba bude mít miliony nebo triliony číslic, ale to na věci nic nemění. Tento triviální "převod" digitálních dokumentů na čísla nám tak nyní umožňuje pracovat s čísly, a nikoli jen s papírovými dokumenty.

Jakákoliv informace, například zvukové cédéčko, digitální záznam zápasu v ledním hokeji, znění zákona o elektronickém podpisu, obsah bankovního příkazu nebo třeba e-mail, bude tedy pro nás od této chvíle pouhým číslem.

Digitální analogie ruční podpisové schopnosti

K tomu, abychom mohli podepsat papírový dokument, potřebujeme kromě pera také **schopnost** vytvořit svůj právoplatný (vlastnoruční) podpis. Tato pro každého člověka jedinečná schopnost umožňuje pořídit náš, sice ne vždy zcela shodný, ale jednoznačně určující, charakteristický podpis na jakýkoliv dokument a za jakýchkoliv okolností. Tato schopnost je složitě zakódována v našem mozku. Je to jen a jen naše soukromá charakteristika, která je (či by alespoň měla být) pro jiné osoby nedostupnou (tajnou) informací.

Podobně pro digitální podpis budeme používat také nějakou soukromou (tajnou) informaci, kterou vlastníme jenom my a nikdo jiný, a tato informace (číslo) bude reprezentovat naši schopnost vytvořit digitální podpis. Toto číslo proto budeme dále nazývat "(tajné) podepisovací číslo" nebo také "(tajný) podepisovací klíč".

Digitální podpis je hračka

Nyní si představme, že podepisujeme papírový dokument. Vezmeme pero a na papír napíšeme svůj podpis. Tím, že na papír naneseme inkoust určitým způsobem, který je jedinečný jen pro nás, **spojíme** hmotné věci, tedy papír a inkoust, s věcí zcela nehmotnou – se svou jedinečnou schopností se podepsat a s konkrétním projevem této schopnosti (vyjádřené konkrétním jedinečným podpisem). U digitálního podpisu to probíhá velmi podobně. Místo papírového dokumentu zde máme číslo reprezentující digitální dokument a místo podpisové schopnosti máme teď tajné podepisovací číslo.

Určitým matematickým spojením těchto dvou čísel vzniká číslo nové, a tím je právě digitální podpis. Vše tedy probíhá stejně přirozeně jako u podpisu ručního. Proces spojení inkoustu s papírem při ručním podpisu je v případě digitálního podpisu nahrazen procesem **spojení dvou čísel** (digitálního dokumentu a tajného podepisovacího klíče) složitými matematickými operacemi. Toto spojení je schopen provést, jak jsme již uvedli, pouze počítač, protože je to velmi složitý výpočet.

Číslo reprezentující digitální podpis daného digitálního dokumentu má mnoho zajímavých a výhodných vlastností. Například digitální dokument se podpisem nijak nemění, na rozdíl od papírového dokumentu, který je při podpisu "umazán" inkoustem. DP je také možné uložit nebo elektronicky přenášet mimo vlastní dokument. Ale hlavně: DP je **nepřenosný** na jiný digitální dokument! Je totiž závislý na každém bitu digitálního dokumentu, k němuž náleží. Pokud podepisujeme (byť v jediném bitu) odlišné digitální dokumenty, jejich digitální podpisy budou naprosto odlišné (nikoliv

jen v jediném bitu). Tuto vlastnost zaručují právě výše uvedené matematické operace provádějící spojení tajného čísla s digitálním dokumentem. Jinými slovy, **digitální podpis má lepší vlastnosti než ručně psaný podpis** – ten je totiž pokaždé stejný (a tedy snadno zfalšovatelný), zatímco DP je na každém dokumentu jiný.

Ověření pravosti digitálního podpisu

Ověřujeme-li pravost rukou psaného podpisu na nějakém dokumentu, máme většinou k dispozici podpisový vzor dotyčné osoby. Jestliže porovnáváme rukou psaný podpis s podpisovým vzorem, neprovádíme otrocké srovnání čar obou podpisů na papíře bod po bodu, ale srovnání obecnějších charakteristik. Koneckonců, nikdo se nedokáže podepsat dvakrát zcela stejně, i kdyby si dal sebevíce záležet. A dále, i když máme k dispozici něčí podpisový vzor, nezískáváme tím ještě **schopnost** takový podpis vytvářet (nemyslí se tím možnost několikrát podpis nějak zfalšovat, ale získat schopnost se takto podepisovat vždy a za každých okolností).

U digitálního podpisu probíhá ověřování podpisu podobně. Naším "podpisovým vzorem" pro ověření digitálního podpisu bude opět číslo, které můžeme nazvat ***veřejným ověřovacím číslem (klíčem)***. Toto ověřovací číslo je sice pevně svázáno s číslem podepisovacím, ale **může být dáno veřejně k dispozici**, stejně jako podpisový vzor u ručního podpisu. Podobně jako podpisový vzor ručního podpisu, nedává toto číslo nikomu schopnost digitální podpis vytvářet, ale pouze ho ověřovat. To opět zajišťuje matematika v pozadí, která umí použít takové operace, jejichž inverze je velmi složitá (tzv. jednosměrné funkce). Ověření digitálního podpisu pak probíhá opět určitým, přesně definovaným spojením digitálního podpisu a veřejného ověřovacího klíče. Výsledkem tohoto spojení je **číslo, které je přímo dokumentem, jenž byl podepsán**. Zmíněné "spojení" je samozřejmě zase složitá matematická operace, kterou opět musí provádět počítač.

Komu věřit?

Podle toho, co víme, si teď představme, jak funguje digitální podpis na internetu. Abychom mohli podepisovat na internetu, vystavíme si zde svůj veřejný ověřovací klíč a uvedeme k němu osobní údaje, které nás jednoznačně identifikují (třeba e-mail, jméno a příjmení, zaměstnání, bydliště, fotografii apod.). Od této chvíle můžeme digitálně podepisovat e-maily, objednávat si zboží za miliony apod. A co příjemce takové objednávky? Ten si z internetu může stáhnout náš ověřovací klíč a ověřit, že náš digitální podpis na milionové objednávce souhlasí. Kde ale vezme jistotu, že osobní údaje, které byly jen tak volně přiloženy k podpisovému vzoru, jsou opravdu naše a nejsou podvržené? Jinými slovy – někdo mu musí **právně zaručit**, že osobní údaje a veřejný ověřovací klíč patří k sobě. V případě digitálních podpisů je to úlohou tzv. certifikátů. ***Certifikát*** je digitální dokument, v němž jsou kromě jiného (například čísla certifikátu, doby platnosti od – do, ověřovací metody apod.) uvedeny zejména údaje identifikující příslušnou osobu a její veřejný ověřovací klíč. Tento digitální dokument je pak digitálně podepsán ***certifikační autoritou***, a to dohromady dává žádaný podepsaný certifikát.

Tím se dostáváme k otázce, jak máme důvěřovat certifikační autoritě? K tomu nás opravňuje právě zákon o EP. Certifikační autorita je totiž podle zákona úřad, který je k vydávání certifikátů zmocněn. Ani u certifikační autority není problém si ověřit, že její veřejný ověřovací klíč patří opravdu k ní. Mimochodem, předpokládá se, že certifikačních autorit v ČR nebude příliš mnoho. Problém důvěry v certifikační autority by tedy neměl vůbec nastat a CA dává prostřednictvím certifikátu právní záruku

spojení osobních údajů s ověřovacím klíčem. Cesta k digitálnímu podpisu je tedy z právního hlediska otevřena.

Certifikační autorita a ověřovatel informací

V komerčním světě se vytvářejí různě složité hierarchie certifikačních autorit. Těží se přitom z tzv. “tranzitivity důvěry”, což znamená, že když domácí certifikační autorita podepíše ověřovací klíč jiné certifikační autority, mohou všichni domácí uživatelé věřit všem certifikátům vydaným cizí certifikační autoritou. Jedná se tedy o pružný systém – ale běda, když jeden článek selže. Náš zákon to řeší “sázkou na spolehlivost”, tranzitivita důvěry v něm tedy není a priori zaručena.

Dále, pro certifikát se zavádí obecnější pojem “osvědčení” a pro certifikační autoritu pojem “ověřovatel informací”. Ověřovatel informací nemůže podle zákona vykonávat žádnou jinou činnost (až na výjimky) než vydávat osvědčení. Kromě řady technických povinností k zajištění bezpečnosti zákon také jasně říká, že ověřovatel informací **musí** před vydáním osvědčení **bezpečně zjistit identitu žadatele o osvědčení**.

Úřad pro elektronický podpis

Z předchozího je zřejmé, že certifikační autorita bude mít významné právní postavení (z laického pohledu to bude něco jako notář specializovaný jen na určité právní úkony). K jejímu schválení proto dojde, jen když bude splňovat zejména bezpečnostní podmínky. Minimálně musí být chráněn její tajný podepisovací klíč, který má cenu notářského razítka a podpisu. Aby to mohlo fungovat, bude muset existovat nějaký úřad, který jmenuje certifikační autority, vydává vyhlášky pro konkrétní provádění zákona a bdí nad dodržováním zákona v oblasti elektronického podpisu. Tento úřad má být zřízen v rámci Ministerstva dopravy a spojů – neměl by však vzniknout rozbujelý aparát a věříme, že se bude jednat o úřad ve smyslu funkčním.

Ještě pár poznámek

Zde bychom mohli skončit, neboť je právě vhodný čas prostudovat si znění zákona a poté se vrhnout do přípravy elektronického obchodu nebo do přípravy digitálních občanských, řidičských a zdravotních průkazů. Možná však nebude na škodu ještě několik drobných poznámek.

• Především – každý občan může mít libovolný počet certifikátů, a to od různých certifikačních autorit (vždy s jinou dvojicí klíčů tajný – veřejný). Je to obdoba dnešních různých průkazů, vydaných k různému typu použití různými vydavateli.

• Certifikát se bude vydávat vždy jen konkrétní osobě (i když může mít jakoukoliv funkci). Například nebude možné vydat certifikát na osobu “Super Banka, a. s.”, ale jen na konkrétní osobu takto: “Josef Novák, jednatel Super Banky, a. s.”.

• Časová omezení certifikátů a jejich on-line dostupnost a odvolatelnost by měla řešit běžné události, jako je odvolání nebo střídání osob ve funkcích apod.

• Jakmile bude zákon přijat, státní správa bude nucena na něj reagovat vytvořením podmínek pro to, aby s ní občan mohl komunikovat elektronicky s využitím svého práva také se elektronicky

právoplatně podepsat (a konečně tedy na úřady nechodit s papíry). V tomto smyslu asi návrh zákona není zase tak úplně apolitický, i když jeho primárním účelem je podpořit elektronický obchod.

• Dále je dobré si uvědomit, že v současném bankovnictví převládá prostý elektronický podpis a jen výjimečně je použita technologie, která bude moci být považována za ZEP. Doufejme, že zákon vytvoří tlak na to, aby se tyto méně bezpečné metody změnily v zaručený elektronický podpis.

• A úplně nakonec poznámka pro detailisty: V článku určeném pokud možno pro nejširší čtenářskou obec bylo nutno uchýlit se k některým zjednodušením. Bylo tak například zamlčeno, že ve skutečnosti se digitálně podepisuje ne přímo příslušný dokument, ale jeho hašovací hodnota; pozorným čtenářům Chipu (např. čísel 3/99 a 4/99) to však jistě neuniklo.

Závěr

Sdružení pro informační společnost (SPIS) se rozhodlo podat státu pomocnou ruku a iniciovalo vypracování paragrafovaného znění zákona o elektronickém podpisu. Pokud bude zákon schválen, z hlediska jeho kvality i možností, které z něj vyplývají, se staneme nejpokrokovější zemí v Evropě. Navrhovaným zákonem stát vytvoří legislativní rámec pro nejrůznější technická řešení. Potom bude řada na informačním a telekomunikačním průmyslu, aby občanům, firmám a obchodníkům nabídl zajímavé služby využívající elektronický podpis. Nic pak také už nebude bránit tomu, aby byla zmodernizována státní správa a povedlo se reálně naplnit i takové vize, jaké jsme např. nabídli v článku "Až nás podepíše počítač", uveřejněném v Chipu 5/99. Pokud by se to podařilo, mohlo by to pozitivně změnit i náš každodenní životní styl.

Vlastimil Klíma (vklima@decros.cz)

Proč nový zákon

Používání moderních telekomunikačních prostředků (elektronické pošty, elektronické výměny dat, ale i telefaxů a jiných prostředků umožňujících dálkové provádění obchodních transakcí) se s rozvojem "informační dálnice" rapidním tempem zvyšuje. Komunikace sdělující závažné informace formou netištěných zpráv však může narazit na překážky v právní oblasti, které by zabraňovaly jejímu používání či by mohly vyvolat námitky ohledně důkazní hodnoty.

Nedostatečná národní legislativa tak vytváří překážky pro mezinárodní obchod, jehož výrazná část se realizuje právě prostřednictvím moderních telekomunikačních prostředků. Stejně negativně působí rozdíly mezi národními legislativami a rozpory při jejich výkladu ohledně používání těchto prostředků.

V českém právním řádu dnes neexistuje jednotná právní úprava, která by jednoznačně připouštěla nebo jednoznačně zakazovala elektronickou formu dokumentace ve všech případech lidského konání. Základní právní normou, která by mohla mít vztah k elektronickému obchodu, je především zákon č. 40/1964 Sb., Občanský zákoník (ObčZ), který v § 40 uvádí: "*Nebyl-li právní úkon učiněn ve formě, kterou vyžaduje zákon nebo dohoda účastníků, je neplatný. Písemně uzavřená dohoda může být změněna nebo zrušena pouze písemně. Písemný právní úkon je platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé. 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.*"

Za splnění podmínky identifikace a autentizace (se současným požadavkem na dodržení principu neodmítnutelnosti) lze provést elektronickou transakci například v prostředí internetu tak, aby splňovala podmínky ust. § 40, odst. 4 ObčZ, zejména "*...určení osoby, která právní úkon učinila*".

Požadavek zajištění identifikace (určení, kdo nějaký projev vůle učinil) a autentizace (ověření totožnosti osoby) vznikl v podstatě ve stejném okamžiku, kdy došlo k zachycení právního úkonu na nějaké záznamové médium. Právní úprava i praxe dospěly posléze k určitým všeobecně uznávaným způsobům a formám používaným v případech, kdy je úkon činěn na papíře. K identifikaci zde slouží nejčastěji vlastnoruční podpis, k němuž jsou připojeny některé osobní údaje (např. jméno, příjmení a rodné číslo), autentizace se uskutečňuje například legalizací, kterou provádí notář nebo příslušný orgán veřejné správy.

Jakmile však začneme chápat pojem "dokument" jinak než pouze v klasické, písemné formě, je zřejmé, že s těmito tradičními nástroji nevystačíme. (Právní řády mnohých států, Českou republiku nevyjímaje, dnes umožňují, aby dokumenty byly již ve své původní podobě vytvořeny i jinak než ve formě listiny, zejména pomocí výpočetní techniky.) V současné době již nečiní potíže provést digitalizaci písemného dokumentu (ve formě "obrázku", tj. coby faksimile) a přitom přenést i podpis, který je na dokumentu učiněn. Samozřejmě že pravost podpisu může být zpochybněna a následně prokazována (např. znalecky). Totéž ovšem platí i o podpisech na listinných dokumentech. Mimo to může být rovněž zpochybněno, zda v průběhu digitalizace nedošlo ke změně obsahu dokumentu – jinak řečeno k tomu, že podpis je sice pravý, ale digitalizovaná podoba obsahu dokumentu se liší od té, která byla původně identifikována a autentizována. I tento důkaz by bylo pravděpodobně možné pomocí bezpečnostních postupů spojených s digitalizací opatřit.

Ještě složitější situace vzniká, pokud je dokument vytvářen přímo prostředky výpočetní techniky, tedy nikoliv jako digitální faksimile, ale přímo jako "počítačová forma" dokumentu (posloupnost jednotlivých znaků zpracovatelných běžným textovým editorem). V zásadě i zde by bylo možno z technického hlediska opatřit dokument podpisem, jde však o to, jak zajistit, aby tento podpis mohl fungovat jako nástroj identifikace a mohla být na jeho základě provedena autentizace.

Možnosti jsou v podstatě dvě: buď zvláštní zákon o elektronickém obchodu, nebo zakotvení elektronického podpisu v českém právním řádu. V obou případech jde prakticky o totéž: učinit dokumenty a podpisy na papíře i v elektronické formě rovnoprávnými.

S první cestou úzce souvisí "Vzorový zákon o elektronickém obchodu" Komise OSN pro mezinárodní obchodní právo (UNCITRAL), která je od roku 1966 Valným shromážděním OSN pověřena harmonizací a unifikací v této oblasti práva. Klíčová myšlenka zákona, totiž že informaci nelze upřít právní důsledky, platnost nebo vykonatelnost jen proto, že má formu datové zprávy, je nepochybně převratem v doposud omezeném chápání dokumentů jakožto informací výlučně spjatých s papírovým nosičem. Základním principem je, že datové zprávy nesmějí být diskriminovány, tj. že nesmí existovat rozpor v zacházení mezi datovými zprávami a dokumenty na papíře.

Začlenění zákona o elektronickém obchodu do našeho právního řádu by vytvořilo kýžené legislativní podmínky pro opravdový, nikoliv jen očekávaný rozvoj elektronického obchodování. Tak rozsáhlý zákon by si však vyžádal poměrně značné množství legislativních prací, a to jak na zákonu samém, tak na platných právních normách souvisejících.

Druhou možností, která neklade tak velké nároky na legislativní proces (přičemž podle názoru předkladatelů i tak vytvoří dostatečné podmínky pro elektronické obchodování), je zakotvení elektronického podpisu v naší legislativě.

V našem návrhu už je použit širší pojem “elektronický podpis” místo původního “digitální podpis”, protože UNCITRAL v loňském roce změnil svůj přístup směrem k méně technologicky závislým právním normám (“elektronický podpis” může být v podstatě realizován jakoukoliv technologií – od naskenovaného podpisu na papíře až k digitálnímu podpisu využívajícímu kryptografických metod).

Ve vyspělých zemích je digitálnímu – nyní elektronickému – podpisu věnována pozornost už dlouhou řadu let. V roce 1998 byl na půdě UNCITRAL zpracován Návrh jednotných pravidel o elektronických podpisech a v témže roce byl schválen Návrh směrnice Evropského parlamentu a Rady pro účely systému elektronických podpisů. Klíčový je pojem elektronického podpisu. Ve smyslu zmíněných dokumentů jej můžeme vymezit tak, že jde o **údaje v elektronické podobě, které jsou připojené nebo logicky spojené s datovou zprávou a které jsou použity ke zjištění totožnosti oprávněné osoby ve vztahu k datové zprávě.**

V praxi je důležité, aby tento podpis byl tzv. **bezpečný,** resp. **zaručený**. Tak je tomu tehdy, když může být ověřen pomocí nějakého bezpečnostního postupu, což má zajistit, že **takový podpis může být použit k identifikaci osoby, která jej vytvořila a oprávněně použila v souvislosti s danou informací, je vzhledem k této osobě jednoznačný a je k informaci připojen buď držitelem podpisu, nebo takovými způsoby, které jsou pod jeho kontrolou.**

Na rozdíl od pouhého elektronického podpisu je účelem zaručeného (bezpečného) elektronického podpisu zajistit, že zprávu podepsala opravdu oprávněná osoba. Vychází z principu existence “ověřovatele informací”, který ověřuje vztah mezi zaručeným elektronickým podpisem a oprávněnou osobou. (Tento termín nahrazuje dřívější “certifikační autoritu”, protože se nemusí jednat jen o správce digitálních podpisů, ale např. i o databanku snímků duhovek oka, vzorců DNA apod.) Dnes je pravděpodobně jedinou reálnou variantou zaručeného elektronického podpisu podpis digitální, vycházející z principu existence dvou klíčů vygenerovaných majitelem podpisu: soukromého (tajného) a veřejného.

Česká republika prozatím právní úpravu elektronického podpisu nemá, byť se již některé firmy pokoušejí jako ověřovatelé informací působit. Zejména vzhledem ke stále rostoucímu objemu a důležitosti vztahů realizovaných prostřednictvím internetu je však nejvyšší čas zareagovat na nové podmínky i právně. Existence elektronického podpisu v české legislativě by však umožnila i výkon některých prvků veřejné správy dálkovým způsobem. Přitom je třeba brát v úvahu skutečnost, že k identifikaci a autentizaci se bude v nepříliš vzdálené budoucnosti používat i jiných prostředků, než je elektronický podpis (digitální otisk prstu nebo duhovky oka).

Z tohoto důvodu byl v rámci SPIS vytvořen návrh zákona o elektronickém podpisu, který také vymezí práva a povinnosti jednotlivých subjektů, a především začlení do ust. § 40 ObčZ alternativní možnost k podpisu na papíře, totiž datovou zprávu podepsanou elektronicky podle zvláštních předpisů. Snahou předkladatelů je, aby byl co nejobecnější a technologicky pokud možno nezávislý, neboť při každé změně technologie by jinak bylo třeba měnit text zákona.

Hlavním cílem zákona je umožnit provádění elektronického obchodu i jiných právních úkonů prostřednictvím moderních informačních či komunikačních technologií a zajistit tzv. “funkčně ekvivalentní přístup”, tedy stejné zacházení jak uživatelům podkladů v tištěné, tak i v elektronické podobě. Vždyť forma, kterou je určitá informace prezentována či uchovávána, nemůže být důvodem, pro který by tato informace pozbyla právní platnosti. Součástí návrhu je i zřízení orgánu státní správy, který bude vykonávat dozor nad ověřovateli informací.

Návrh zákona vznikl díky iniciativě SPIS a některých poslanců Parlamentu ČR, kteří hodlají tento návrh prosadit cestou poslanecké iniciativy, když práce prováděné v tomto směru ÚSIS probíhaly

dlouho a nepříliš úspěšně. Autory návrhu jsou doc. Vladimír Smejkal a doc. Pavel Mates. Zákon v paragrafovaném znění byl 23. 9. nabídnut k veřejné diskusi a po zapracování připomínek má být koncem října předložen vládě ČR jako poslanecká iniciativa místopředsedů čtyř politických stran: Ivana Langra za ODS, Stanislava Grosse za ČSSD, Vladimíra Mlynáře za US a Cyrila Svobody za KDU ČSL.

Vladimír Smejkal