

Uveřejněno v časopise Právní rádce, XII., 2004, č. 12, s. 9 – 14.
Jakékoliv užití tohoto článku jinak, než pro vlastní potřebu, stejně jako šíření textu nebo jeho částí jakýmkoliv způsobem, je přísně zapovězeno!

Elektronický podpis po novele zákonem č. 440/2004 Sb.

Elektronický podpis, který již trvale zakotvil v českém právním řádu, je definován zvláštním zákonem včetně aktualizovaných prováděcích předpisů. Novelami tohoto zákona i jiných zákonů souvisejících se začínají vytvářet stále pevnější základy pro elektronický výkon veřejné moci, tzv. e-government. Škoda, že v soukromoprávním užití převažuje nasazování elektronického podpisu pouze v interních aplikacích, zatímco např. při vzniku závazkových vztahů mezi podnikateli je tato cesta, a to především z důvodu obavy z dokazování v případných soudních sporech, opomíjena.

Učený kolega Tomáš Sokol se ve svém zajímavém článku zabývá problematikým vnímáním a výkladem základního stavebního kamene právních aktů, jakým je podpis, přičemž se zabývá převážně podpisy na papíru, případně jiných „neelektronických“ nosičích. V závěru pak vyslovuje obavu, že lze zejména při narůstající elektronizaci komunikace očekávat výkladové problémy.

Osobně se domnívám, že používání různých druhů a způsobů podepisování v našem právním řádu je již teď natolik zmatené, včetně hypertrofického požadavku na úředně ověřený podpis za situace, kde to je zjevně nepřiměřené nebo dokonce tam, kde je požadavek na úřední ověření nápadem osoby soukromého práva při ryze soukromoprávním úkonu (typicky touto fobií trpí některé banky). Naopak užívání elektronického podpisu, který je velmi podrobně popsán v zákoně č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů, je z hlediska jednoznačnosti výkladu snadnější, ačkoliv zde přetrvávají různé psychologické, nikoliv však faktické bariéry.

Co ovšem znesnadňuje používání elektronického podpisu při komunikaci s orgány veřejné moci, alespoň některými, je absence jednotné právní úpravy podávání a doručování v českém právním řádu, přičemž naprostý primát vítězství třímá cyklické povolování a zakazování ryze elektronického podání občanským soudním řádem. V českém právním řádu existují více než tři desítky odlišných právních úprav základních procesních úkonů, jako jsou podávání, doručování, předvolávání apod.,¹ řešením by byl jednotný „Zákon o podávání a doručování“, který je odmítán resorty, jež se nechtějí smířit s myšlenkou opuštění partikulárních úprav v jednotlivých procesních normách² nebo i v dalších právních předpisech,³ jež – bohužel – spadají do působnosti různých gestorů, tj. ministerstev a dalších ústředních správních orgánů.⁴ V této oblasti se sice rýsuje možnost společné iniciativy ministra – předsedy Legislativní rady vlády a ministra informatiky, směřující k vytvoření takového zákona,

¹ Smejkal, V.: Doručování v českém právním řádu. Justiční praxe. L., 2002, č. 10, s. 572 – 603

² Jako jsou občanský soudní řád (zákon č. 99/1963 Sb.), soudní řád správní (zákon č. 150/2002 Sb.), trestní řád (zákon č. 141/1961 Sb.), správní řád (zákon č. 500/2004 Sb.), zákon o správě daní a poplatků (zákon č. 337/1992 Sb.) apod.

³ Např. v zákoníku práce, v zákonu č. 40/2004 Sb., o veřejných zakázkách apod.

⁴ V této oblasti se sice rýsuje možnost společné iniciativy ministra – předsedy Legislativní rady vlády a ministra informatiky, směřující k vytvoření takového zákona, nicméně je otázkou, nakolik se to podaří ještě ve volebním období stávajícího Parlamentu.

nicméně je otázkou, nakolik se to podaří ještě ve volebním období stávajícího Parlamentu.

Elektronické podepisování se nicméně objevuje v nových právních předpisech a aktualizovaných zněních předpisů stávajících, a lze doufat, že všichni předkladatelé již nebudou zapomínat ve svých legislativních návrzích na oba rovnocenné způsoby možné komunikace, tj. v listinné podobě, opatřené klasickými podpisy, a v podobě elektronické, s využitím zmíněného elektronického podpisu.

Princip elektronického podpisu

Přestože problematika elektronického podpisu byla již na stránkách Právnického rádce popsána,⁵ bude vhodné si zopakovat alespoň základní princip. Mějme dokument v elektronické podobě, který je tedy tvořen posloupností digitálních nul a jedniček, tedy můžeme jej chápat jako jedno, byť hodně dlouhé číslo. Dále máme svůj *tajný (soukromý) klíč*, což je opět posloupnost digitálních nul a jedniček, tedy také jakési číslo. Zjednodušeně řečeno, elektronický podpis spočívá v tom, že program pro podepisování (což může být např. MS Outlook) obě čísla spolu zkombinuje. Výsledkem řady složitých matematických operací je třetí číslo, a to je právě elektronický podpis.

Důsledkem tohoto postupu jsou dvě skutečnosti: 1. elektronický podpis není konstanta, kterou byste si někde „vyfasovali“, jak např. mylně tvrdí Ministerstvo informatiky, údajně proto, aby výklad ještě více zjednodušilo; 2. změní-li se byť jen jediná nula či jednička, tedy např. jeden znak v podepisovaném dokumentu, změní se i výsledek výpočtu, tj. elektronický podpis. Odborněji řečeno, elektronický podpis je funkcí obsahu dokumentu a soukromého klíče. Jelikož soukromý klíč zůstává konstantní, mění se podpis při každé změně podepisovaného dokumentu.

Zákon takovýto podpis, který splňuje následující požadavky: 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat, nazývá *zaručeným elektronickým podpisem*.

Elektronický podpis nám proto poskytuje daleko vyšší míru zabezpečení, než podpis na papíru, a to i když je úředně ověřený. Dokument, jednou podepsaný elektronicky, je prakticky navždy chráněn proti padělání. Přitom obsahem elektronického dokumentu, resp. jak říká zákon *datové zprávy*, mohou být jakákoliv elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou – tedy text, obrázek, fotografie, film, audiovizuální soubor, počítačový program atd., prostě cokoli, co lze digitalizovat.

Abychom si mohli ověřit, zda je podpis platný, musíme ale provést zase jinou matematickou operaci (resp. sled operací, které za nás automaticky provede opět počítačový program). Příjemce nebo ten, kdo si chce ověřit platnost elektronického podpisu, má totiž k dispozici třetí číslo – tím je tzv. veřejný klíč, opět posloupnost nul a jedniček, která je komplementární ke klíči soukromému. Oba klíče tvoří navzájem se doplňující dvojici, přičemž z jednoho nelze odvodit druhý. Při ověření pravosti elektronického podpisu zadáme do programu dokument obsahující ověřovaný podpis

⁵ Smejkal, V.: Elektronický podpis. Legislativa elektronické komunikace. Právnický rádce, VIII., 2000, č. 2, s. 5-7 resp. Smejkal, V.: Elektronický podpis v praxi. Právnický rádce, IX., 2001, č. 1, příloha s. I-VII

a veřejný klíč, program provede bleskurychle výpočet a sdělí nám coby odpověď jednu ze dvou variant: a) podpis je v pořádku, dokument podepsala osoba, již patří veřejný klíč, a dokument nebyl od okamžiku vytvoření podpisu změněn; b) pozor – něco není v pořádku: buď dokument podepsala jiná osoba nebo byl následně po podepsání dokument změněn.

Elektronický podpis nechrání dokument proti padělání, ale umožňuje, že padělání bude možno zjistit. Pokud by příjemce ověření neprovedl, pak se samozřejmě informaci o pravosti podpisu a dokumentu nedozví. Elektronický podpis neslouží ani k utajení obsahu dokumentu: podepsaný dokument je stále „otevřený“ a pokud chceme utajit jeho obsah, musíme použít jiný kryptografický postup, a to *šifrování*. Ale to je jiná otázka.

Problémem, který bylo třeba vyřešit, je, jak se dostane veřejný klíč k příjemci, který může být třeba na druhém konci světa a tedy mu jej nemůžeme předat osobně. Pokud bychom jej poslali např. na disketě poštou nebo jako soubor připojili do e-mailu, mohl by útočník zaměnit obsah zásilky, vyměnit v ní náš veřejný klíč za svůj a pak posílat příjemci svoje podepsané správy, přičemž příjemce by se domníval, že jde o zprávy podepsané námi. Proto se používá elektronické potvrzení o veřejném klíči neboli tzv. *certifikát*. To je elektronický dokument, který obsahuje již zmíněný veřejný klíč, údaje o tom, komu tento klíč patří, případně další údaje o majiteli klíče podobně, jako je najdeme např. v občanském průkazu nebo ve výpisu z obchodního rejstříku. A aby nemohl tento certifikát útočník padělat, osoba, která se zabývá vystavováním certifikátů (*poskytovatel certifikačních služeb*) jej podepíše svým elektronickým podpisem. Tento certifikát potom můžeme posílat e-mailem, vystavit jej na svých webových stránkách, nosit v přenosné paměti (tzv. flash paměti) nebo na čipové kartě s sebou apod. Kdokoliv může znát náš veřejný klíč a mít certifikát; nikdo nikdy se ale nesmí dostat ke klíči soukromému, neboť by se mohl pak do ukončení platnosti certifikátu kdykoliv podepsat za nás.

Certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty, se nazývá *kvalifikovaný certifikát*. Celý zákon o elektronického podpisu a záruky z něj vyplývající se také více méně vztahují na zaručený elektronický podpis a kvalifikovaný certifikát.

Zákon dává následující záruky: 1. soulad s požadavky na podpis – použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu; 2. soulad s originálem – použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit.

Podepisující osobě i poskytovateli certifikačních služeb, zejména těm, kteří vydávají kvalifikované certifikáty, ukládá zákon řadu povinností, přičemž porušení těchto povinností může zavdat jednak správní postih dozorovým orgánem, kterým je Ministerstvo informatiky, podle tohoto zákona, ale také zde vzniká odpovědnost za škodu způsobenou porušením povinností podle zvláštních právních předpisů (tj. podle občanského zákoníku).

Pro komunikaci s orgány veřejné moci zákon předepisuje ještě náročnější variantu. Nestačí pouze vytvořit zaručený elektronický podpis s využitím kvalifikovaného certifikátu, ale podle ust. § 11 zákona v oblasti orgánů veřejné moci je možné za

účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané *akreditovanými poskytovateli certifikačních služeb* (neboli tzv. „uznávaný elektronický podpis“). Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Podle vyhl. č. 496/2004 Sb., o elektronických podatelnách, údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295 a je spravován ústředním orgánem státní správy. Jeho hodnota není zaměnitelná s rodným číslem a nesmí být osobním údajem podle zvláštního právního předpisu (tj. podle zákona o ochraně osobních údajů). Tento tzv. bezvýznamový identifikátor zatím není konkrétně definován, nicméně je veřejným tajemstvím, že by to mělo být číslo sociálního pojištění, vydávané Českou správou sociálního zabezpečení.

Akreditovaný poskytovatel certifikačních služeb je u nás zatím jediný (od 18.3.2002 je jím První certifikační autorita, a.s. – viz www.ica.cz), ale údajně požádal po více než dvou letech další žadatel, což by mohlo vést k žádoucímu konkurenčnímu boji na tomto velice úzkém trhu.

Novela zákona o elektronickém podpisu

Dnem 26. července 2004 nabyl účinnosti zákon č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Kromě *časového razítka*, které je již ve světě používáno, leč ne všude kodifikováno, zavedl do našeho právního řádu dvě důležité novinky, které mají vztah především k činnosti orgánů veřejné moci. Jsou to tzv. *elektronická značka* a *elektronická veřejná listina*.

Elektronická značka je vlastně elektronický podpis vytvořený technickým zařízením. Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu; 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou; 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat. (Přitom kvalifikovaný systémový certifikát je obdoba dříve popsaného kvalifikovaného certifikátu. Ten ale může být vydán nikoliv jen fyzické osobě, ale jakémukoliv majiteli označujícího zařízení, tj. i osobě právnické.)

Rozdílem je právě to, že značka není podpis, protože je vytvářena technickým zařízením, automatizovaně.⁶ Nejedná se o podpis ve smyslu občanského zákoníku, neboť jej nevytvořila fyzická osoba, ale „ne-osoba“. Definičně, resp. funkčně jde ale o totéž. Podepisující osobu nahradí tzv. označující osoba, což je fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou pomocí prostředku pro vytváření elektronických značek, který musí být nastaven tak, aby i

⁶ Podle občanského zákoníku, jakožto obecného právního předpisu, může právní úkon jehož součástí je podpis učinit pouze a jen fyzická osoba. Právní úkony právnické osoby činí ti, kteří k tomu jsou oprávněni smlouvou o zřízení právnické osoby, zakládací listinou nebo zákonem (statutární orgány), případně další osoby (jiní její pracovníci nebo členové), pokud je to stanoveno ve vnitřních předpisech právnické osoby nebo je to vzhledem k jejich pracovnímu zařazení obvyklé. Jinými slovy – podepsat, a to ani elektronicky, se nemůže sama právnická osoba (např. banka či stát), nemůže se ale podepsat ani technické zařízení bez lidské obsluhy.

bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí. (Tím se nemyslí tedy provádění úkonu, vztahujícího se ke každé zprávě, fyzickou osobou, jako tomu je u elektronického podpisu, ale nastavení určitého pravidla – algoritmu, kterým bude prostředek řízen.) Prostředek pro vytváření elektronických značek, tj. ve skutečnosti počítač, musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

Druhým rozdílem je, že u elektronického podpisu pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila (§ 3 odst. 1 zákona). U značky se vytváří právní fikce opačná, tj. má se za to, že označující osoba označila datovou zprávu bez předchozí kontroly vlastního obsahu datové zprávy (§ 3a odst. 2).

Používání elektronických značek bude přínosné tam, kde je ze zákona nezbytné důvěryhodným způsobem označovat velké objemy datových zpráv v relativně krátkém časovém období (např. proces potvrzování doručení podání učiněného v elektronické podobě na server orgánu veřejné moci) a vytváření zaručeného elektronického podpisu pro každou datovou zprávu by bylo z hlediska časového, personálního a finančního nadbytečně náročné, a dále tam, kde není možné používat kvalifikované certifikáty. Předpokládá se, že elektronické značky budou využívány v agendách týkajících se například celních řízení, při vydávání elektronických výpisů z úředních databází, při potvrzování přijetí elektronických zpráv, při elektronické fakturaci apod.

Za nejpřevratnější moment novely zákona o elektronickém podpisu lze ale považovat ustanovení § 11 odst. 2, který říká: *„Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.“*

Co tento nenápadný textík znamená prakticky? Elektronické značky založené na kvalifikovaných systémových certifikátech a uznávané elektronické podpisy jsou způsobilé zajistit nepopiratelnost původu a originalitu obsahu dat v elektronické podobě, ke kterým jsou připojeny. Proto mohou být plnohodnotnými náležitostmi elektronických písemností orgánů veřejné moci – mají totiž stejnou funkci jako úřední razítko a podpis úřední osoby na listině. Listiny, vydané těmito orgány, se označují jako tzv. veřejné listiny a při úředním resp. soudním jednání se nemusí dokazovat jejich obsah (na rozdíl od listin soukromých). Jakmile budou vytvořeny technicko-organizační podmínky podle zákona, případně dalších zákonů, bude možno získat – již výlučně v elektronické podobě výpisy z různých evidencí spravovaných orgány veřejné moci – např. výpis z Rejstříku trestů, z katastru nemovitostí či obchodního rejstříku. (Pokud tomu nebudou bránit některá kogentní ustanovení právních předpisů, upravujících tyto rejstříky.) Tím by mělo dojít ke skutečnému postupnému prosazování e-governmentu do naší veřejné správy.

Aby bylo možno vydávat takové výpisy v listinné podobě na určených místech a aby si mohly tyto elektronické veřejné listiny vyměňovat orgány veřejné moci, připravují se na Ministerstvu informatiky dva právní předpisy. Je to novela zákona č. 365/2000 Sb. o informačních systémech veřejné správy; tento zákon je ve své podstatě zákonem, především upravujícím činnost Ministerstva informatiky a povinnosti provozovatelů informačních systémů veřejné správy (dále také jen „ISVS“). Novela je zaměřena na aktualizaci postavení ministerstva, jeho práv a povinností, jakož i práv a

povinností orgánů veřejné správy v souvislosti se správou a provozem těchto informačních systémů, ale také zavádí možnost decentralizovaného vydávání ověřených výstupů z ISVS v listinné podobě, které mají vydávat notáři a držitelé poštovní licence (tj. Česká pošta). Kromě toho je nyní projednáván věcný záměr zákona o sdílení dat ve veřejné správě, který má upravit předávání dat mezi registry, tedy plně elektronickými databázemi, jež jsou zdrojem dat v rámci ISVS, komunikaci mezi jednotlivými informačními systémy orgánů veřejné správy (správně by ovšem mělo být vztaženo i na ostatní orgány státu, tj. veřejné moci).

Konečně poslední novinkou v českém právním řádu zavedenou novelou zákona o elektronickém podpisu je *časové razítko*. Časové razítko je nástroj, který hodnověrným způsobem zajišťuje přiřazení aktuálního časového údaje k elektronickému dokumentu. Jinými slovy, můžeme získat důkaz o tom, že určitý elektronický dokument (datová zpráva) existovala v určitý časový okamžik. To může být velice významné v řadě případů: při vyplňování tzv. elektronické doručky, při podávání daňového přiznání nebo nabídky v rámci veřejné zakázky, při sporech o autorská či jiná práva duševního vlastnictví apod.

Toto razítko vznikne tak, že kvalifikovaný poskytovatel certifikačních služeb (v zahraničí označovaný jako tzv. TSA – Time Stamping Authority) elektronicky podepíše dokument včetně k němu připojeného časového údaje a dalších identifikačních údajů. (Ve skutečnosti není podepisován dokument, ale jeho vzorek, neboli zjednodušeně řečeno kontrolní součet – tzv. hash, ale to je na samostatnou publikaci.) Časové razítko neobsahuje identifikaci žadatele, tj. nemůže sloužit jako důkaz o tom, že bezprostředně před okamžikem vydání razítka měla dokument v držení určitá osoba, ale toto lze snadno řešit tak, že bude „orazítkován“ dokument, předtím elektronicky podepsaný držitelem.

Novela zavádí tzv. „*kvalifikované časové razítko*“, což je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. Toto razítko musí dle zákona obsahovat: a) číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb (KPCS⁷), b) označení pravidel, podle kterých KPCS kvalifikované časové razítko vydal, c) označení KPCS, d) hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka, e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno, f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal. (Tím je časové razítko opět chráněno proti padělání či modifikaci.)

Nutno říci, že teprve při psaní tohoto článku jsem si uvědomil jistou past doslovného výkladu této definice, která pravděpodobně vychází z nějakého zahraničního dokumentu, tvořeného technology. Lze totiž diskutovat o tom, jak dlouho data existovala před daným časovým okamžikem – hodinu, týden, rok, desetiletí? Možná by bylo přesnější použít definici jinou, právnicky přesnější, tj. typu „data existovala v okamžiku vytvoření vzorku (hash) dokumentu (k němuž je časové razítko vyžadováno) a jeho doručení k poskytovateli“, případně jednodušší „v okamžiku doručení vzorku dokumentu k poskytovateli“. Ale toto může být dle mého názoru řešeno výkladově, přičemž by se dalo diskutovat i o dalších otázkách, týkajících se časových souvztažností.⁷

⁷ Smejkal, V.: Novela zákona o elektronickém podpisu a časové razítko. Crypto-World, VI., 2004, č. 4, s. 2 – 3

Pojem „kvalifikovaný poskytovatel certifikačních služeb“ zní sice nově, ale jedná se v podstatě do zákona vloženou legislativní zkratku pro osobu, která vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen „kvalifikované certifikační služby“) a splnil ohlašovací povinnost Ministerstvu informatiky podle § 6 zákona.

Poskytovatel, který vydává kvalifikovaná časová razítka, je povinen podle novely zákona: a) zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem, b) zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka, c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku, d) přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek, e) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

Zákon říká v novém § 6b odst. 2, že kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání. Tady samozřejmě očekávám námitky technologických vykladačů práva, co že to je ono „neprodleně“, a je mi jasné, že budou požadovat kvantifikaci, nejlépe s přesností na milisekundy. Neprodleně znamená tak rychle, jak je to jen možné – viz také předchozí připomínka o okamžiku existence „razítkovaných“ dat.

Osobně se domnívám, že stejně bude muset být značně novelizována prováděcí vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu, případně doplněna jinými vyhláškami; tedy je možné v novém znění vyhlášky uložit poskytovatelům časových razítek povinnost, aby do svojí „razítkovací“ prováděcí směrnice napsali, jakou dobu odezvy a jakou přesnost časového údaje zaručují.

Archiv podepsaných dokumentů

Rozhodneme-li se používat elektronicky podepsané dokumenty, budeme postaveni před otázkou, jak prokazovat platnost takto podepsaného dokumentu s určitým časovým odstupem, tj. i v případě, kdy platnost certifikátu, pomocí kterého je možno ověřit pravost podpisu, již vypršela. (Certifikát se nyní vydává na 1, maximálně na 2 roky.) Tato otázka je zřejmě dnes asi pro řešitele technologií pro elektronický podpis největší výzvou, přičemž již existují, a to i u nás, tzv. *důvěryhodné archivy elektronických dokumentů* (TAA – Trusted Archiving Authority), které zajišťují integritu uložených dokumentů a poskytují důkazy o jejich autenticitě jak vůči uživateli, tak vůči třetím osobám. Takový archiv dlouhodobě ošetřuje elektronické podpisy dokumentů a garantuje platnost podepsaných dokumentů po celou dobu archivace, o čemž při jejich vydání archiv poskytuje také nezpochybnitelné důkazy. Dlouhodobě také zabezpečuje obnovu platnosti časových razítek. Ani rychlý vývoj technologií by tedy neměl uživatele elektronického podpisu zaskočit, neboť výrobci udávají, že počítají s úschovou i nad 20 let či dokonce trvale.

Přeshraniční vztahy

Novela současně reaguje na právě probíhající vstup ČR do Evropské unie. Jedná se především o možnost uznávání kvalifikovaných certifikátů v členských státech EU, o možnost získání akreditace k působení jako akreditovaný poskytovatel certifikačních

služeb pro poskytovatele se sídlem v jiném státu a o možnost vydávat kvalifikované certifikáty podle tohoto zákona i v jiném státu.

Co se týká uznávání zahraničních kvalifikovaných certifikátů, pak platí podle novely: (1) Certifikát, který je vydán poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie jako kvalifikovaný, je kvalifikovaným certifikátem ve smyslu tohoto zákona. (2) Certifikát, který je vydán jako kvalifikovaný ve smyslu tohoto zákona v jiném než členském státu Evropské unie, je kvalifikovaným certifikátem ve smyslu tohoto zákona pokud a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie; b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, který splňuje podmínky práva Evropských společenství, převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů; nebo c) to vyplývá z mezinárodní smlouvy.

Další změny zákona o elektronickém podpisu ve většině případů souvisejí s výše popsány novinkami. Výjimkou jsou některá upřesnění, vyplývající z aplikační praxe, případně z nové koncepce legislativy. Jde zejména o správní delikty právnických osob dle usnesení vlády č. 162 ze dne 20. února 2002, kterým vláda schválila koncepci reformy správního trestání a podle níž jsou průběžně upravovány prakticky všechny veřejnoprávní předpisy, kde správní trestání přichází v úvahu.

Závěrem

Domnívám se, že novela umožní další, snad ještě větší pokrok v přechodu na maximálně elektronický výkon veřejné moci, nežli bylo vydání původního znění zákona. Klíčová otázka ale přetrvává již od roku 2000: budou státní orgány podporovat a vytvářet aplikace, které budou s těmito novými prvky pracovat? Nebo budou hledat stále odůvodnění, proč to nejde? Případně: stojí a padá podpora e-governmentu s existencí Ministerstva informatiky, čemuž momentálně vše nasvědčuje?

Co se týká soukromoprávních vztahů a elektronického podpisu, nejsem velkým optimistou. Banky, které jediné mohly masově začít používat elektronický podpis podle zákona, daly přednost svým, byť principiálně někdy podobným proprietární řešením internet-bankingu a home-bankingu. Zdravotnictví je natolik zmítáno vážnějšími problémy, že nelze očekávat zásadní pokrok směrem k čipovým kartám se zdravotnickou dokumentací, kterou by zřejmě používaly nejen velké nemocnice, ale i soukromí lékaři. Některé větší subjekty pracují nebo již používají tzv. infrastrukturu veřejného klíče (PKI – Public Key Infrastructure), ale takřka výlučně pro interní potřebu. Čeká se na nějakého hybatele, který dá impuls k masovému zavádění elektronického podpisu, a domnívám se, že jím může být asi jen stát, který uvažuje o čipových kartách pro zaměstnance státní správy, které by měly sdružovat osobní průkazy, přístupové karty a prostředky pro elektronické podepisování. Jen aby to uvažování netrvalo příliš dlouho.

Vladimír Smejkal, soudní znalec, člen Legislativní rady vlády a člen redakční rady Právního rádce

