

### **Elektronický podpis**

**Nahradí nová technologie klasický vlastnoruční podpis na papíře nebo se jedná jen o prostředek k dalšímu rozvoji sítě Internet a mohutnému postupu elektronického obchodování?**

Pojem elektronického podpisu byl do našeho právního řádu pevně zakotven zákonem č. 227/2000 Sb. ze dne 29.června, o elektronickém podpisu a o změně některých dalších zákonů (dál jen zákon o elektronickém podpisu), který nabyl účinnosti 1.října roku 2000. Tímto zákonem byly vytvořeny základní legislativní pravidla pro používání elektronických podpisů a hlavně jejich zrovnoprávnění s podpisy vlastnoručními. Nicméně technologie, která se při elektronickém podpisu užívá není zase tak převratná. Již v minulosti byla používána v oblasti medicíny, kde se již dříve „podepisovaly“ pomocí této metody některé speciální revidované pokusy nebo postupy, a to za účelem přesné identifikace subjektu, který tyto provedl.

Účelem zákona o elektronickém podpisu je úprava používání elektronického podpisu, poskytování souvisejících služeb, kontrola povinností a sankce za porušení povinností stanovených zákonem. Vývoj k této zákonné úpravě nebyl nijak jedinečný či samostatný, ale je důsledkem působení několika vlivů. Jednak jde o působení Komise OSN pro mezinárodní právo (UNCITRAL), kde vznikl tzv. Vzorový zákon o elektronickém obchodu. Tento vzor má ovšem sloužit pouze jako obecná předloha pro jednotlivé státy, které v důsledku vývoje potřebují tyto technologie a jejich použití upravit a dát jim určité mantinely. Další oblastí, kde došlo k výraznému posunu jsou Evropská společenství. Tady byla v listopadu 1999 vydána Komisí závazná Směrnice č. 1999/93/EC, o zásadách Společenství pro elektronické podpisy. Tato Směrnice je již méně obecná než Vzorový zákon a obsahuje zejména právní rámec, ovšem bez dostatečného technologického popisu a určení konkrétních pravidel. Členské státy Evropské Unie mají od doby přijetí této Směrnice nyní 18 měsíců na to, aby přijaly příslušné právní normy do svých právních řádů a umožnily tak konkrétní užívání v praxi a v elektronickém obchodě.

Směr naznačený Komisí EU převzal i náš zákon o elektronickém podpisu, který byl přijat parlamentem jako legislativní rámec využívání těchto postupů a vlastní technické zabezpečení a pravidla nechává na prováděcích předpisech. Jak již to bývá, jsou tyto prováděcí předpisy zatím pouze v podobě tzv. tezí, které by měly upravit postavení poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty, a jejich smluvních partnerů. Významné postavení v rámci celého zákona je dáno Úřadu pro ochranu osobních údajů (dále jen Úřad), který bude vydávat akreditace pro poskytovatele kvalifikovaných certifikátů.

Pro další výklad je třeba zmínit několik zákonných definic, které i sám zákon o elektronickém podpisu zařadil hned na počátek. Jedná se zejména o pojem tzv. zaručeného elektronického podpisu.

*Zaručeným elektronickým podpisem* jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

Již z tohoto ustanovení docházíme k tomu, že elektronický podpis není nějaký zkopírovaný či naskenovaný vlastnoruční podpis. Naopak daleko více je to pouze soubor dat (dlouhá řada znaků a čísel), který je vytvořen podepisující osobou, a to pomocí klíče a programu nainstalovaného v počítači. Tento klíč se potom použije k zašifrování dokumentu. Osoba příjemce (v případě zájmu i kdokoliv třetí) se může pomocí veřejného klíče, tzv. protikusu k osobnímu klíči, přesvědčit, zda tento použitý kód náleží podepisující osobě a zda nedošlo v zaslaném dokumentu následně po podpisu ke změnám. Dokument, který se elektronicky podepisuje může být textový, obrazový, ale i zvukový aj. Obecně lze říci, že zájemce o elektronický podpis obdrží počítačový software k vytvoření a ověření elektronického podpisu. Za pomoci příslušného software vygeneruje zájemce o elektronické podepisování dva protikusy (soukromý a veřejný klíč). Ten veřejně přístupný klíč předloží poskytovateli identifikačních služeb (certifikační autoritě), která mu na základě jeho osobních údajů vystaví certifikát. Certifikát potom vlastně prokazuje, že určitý veřejný klíč je přiřazen k určité osobě. Příjemce podepsaného dokumentu si může pomocí veřejného klíče ověřit, že datová zpráva byla podepsána konkrétní podepisující osobou.

Co se týče dalších zákonných definic, byla vymezena *datová zpráva*, jako elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou. *Podepisující osoba* je fyzická osoba, která má prostředek pro vytváření podpisů a jedná jménem svým nebo v zastoupení fyzické či právnické osoby. K dalším pojům zákona bych se zmínil o *poskytovatelích certifikačních služeb*, což jsou subjekty, které vydávají certifikáty a vedou jejich evidenci, případně poskytují další služby spojené s elektronickými podpisy. Dále se objevuje pojem *akreditovaný poskytovatel certifikačních služeb*, což je poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle zákona o elektronickém podpisu. *Certifikátem* je datová zpráva, která je vydána poskytovatelem certifikačních služeb a spojuje data pro ověřování podpisu s podepisující osobou a umožňuje ověřit její totožnost. I zde se objevuje pojem *kvalifikovaný certifikát*, což je potom certifikát, který má náležitosti stanovené zákonem o elektronickém podpisu a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty. *Akreditací* se rozumí osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

Pro podepisující osobu jsou stanoveny přímo ze zákona tři základní povinnosti :

1. zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
2. uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu,
3. podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

Za škodu způsobenou porušením těchto povinností podepisující osoba odpovídá podle příslušných ustanovení občanského zákoníku o obecné odpovědnosti za škodu. Vychází se zde z předpokládaného zavinění, a to pouze nedbalostí nevědomou. Poškozený ovšem musí prokázat, že v jednotlivém případě došlo k porušení právní povinnosti (např. že podepisující nezacházel s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití), že vznikla škoda o určitém rozsahu, a že vznik škody je v příčinné souvislosti s porušením právní povinnosti. Již z výše uvedeného ovšem vyplývá, že dokazování je v těchto případech nadmíru obtížné.

Na tomto místě je třeba ještě zmínit činnost Úřadu, který je podle zákona o elektronickém podpisu zmocněn k vydávání prováděcích předpisů. Toto zmocnění vyplývá z ustanovení § 6 a § 17 zákona o elektronickém podpisu, týkajících se povinností poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty. Takový poskytovatel musí používat bezpečné systémy a nástroje elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují. Bezpečnost nástroje elektronického podpisu bude potom ověřena Úřadem. Uvedená vyhláška se pouze objevuje v pracovní verzi a popisuje hlavně technologické a technické postupy, které nejsou obsahem vlastního zákona o elektronickém podpisu. Úřad kromě toho pracuje ještě na další vyhlášce, která bude upravovat postup při hodnocení shody jednotlivých nástrojů elektronického podpisu. Vzhledem k tomu, že v současné době ještě nejsou prováděcí předpisy hotovy, není možné elektronický podpis používat v rámci veřejné správy (viz dále), což je velkou nevýhodou současné praxe. Není tedy ještě umožněno, aby byl elektronický podpis využíván v rámci styku se soudy, finančními úřady či státní správou nebo samosprávou.

V oblasti orgánů veřejné moci je možné dle ustanovení § 11 zákona o elektronickém podpisu používat *pouze* zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (tak jak to vyjadřuje i Směrnice Komise EU). Ovšem v oblasti

soukromoprávních vztahů a pro soukromoprávní subjekty mohou fungovat, a již také dnes fungují, neakreditování poskytovatelé.

V zásadě se tedy rozlišují dvě skupiny poskytovatelů certifikačních služeb. Jedná se o poskytovatele certifikačních služeb vydávající kvalifikované certifikáty, které jsou akreditované Úřadem, a jiní poskytovatelé certifikačních služeb. Pro neakreditovaného poskytovatele je stanovena zákonná povinnost, aby nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu ohlásil Úřadu, že bude vydávat kvalifikované certifikáty. Smyslem tohoto ustanovení je dosažení kontroly nad kvalifikovanými certifikáty a možnost sankcionovat porušení pravidel.

Vlastní technický průběh elektronického podepisování zajišťuje metoda tzv. asymetrické kryptografie, která vytváří již výše zmíněné protikusy (klíč soukromý a veřejný). Z veřejného klíče nijak nevyčteme klíč soukromý, který ovšem pomocí klíče veřejného můžeme ověřit. Veřejný klíč je k dispozici buď přímo od podepisující osoby, poskytovatele certifikačních služeb nebo je volně k dispozici na síti Internet.

Význam elektronického podepisování vyplývá z následujícího shrnutí:

1. Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem - **velký rozsah použití a jednoduchost.**
2. Použití zaručeného elektronického podpisu, který je založen na kvalifikovaném certifikátu a který je vytvořen pomocí prostředku pro bezpečné vytváření podpisu, umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na kvalifikovaném certifikátu – **identifikace konkrétní podepisující osoby.**
3. Použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit – **kontrola integrity obsahu a důkaz o tom, že podepisující osoba konkrétní dokument podepsala.**

Zákon o elektronickém podpisu novelizoval také řadu důležitých předpisů. Mezi ty nejzákladnější patří novelizace ustanovení § 40 občanského zákoníku (zákon č. 40/1964 Sb., ve znění změn a doplňků) o právních úkonech. Nové znění odst. 3 nyní umožňuje, aby právní úkon, který je učiněn elektronickými prostředky, byl i elektronicky podle zvláštních předpisů podepsán. Zákon o správě daní a poplatků (zákon č. 337/1992 Sb., ve znění změn a doplňků), nyní umožňuje ve svém § 21 odst. 3, aby daňové subjekty mohly podepsat elektronicky správci daně tiskopisy, které jsou zveřejněné v elektronické podobě. Také občanský soudní, trestní a správní řád, (zákony č. 99/1963 Sb., č. 141/1961 Sb. a č. 71/1967 Sb. vždy ve znění změn a doplňků), mají novelizovaná ustanovení týkající se podání, která lze nyní učinit i v elektronické podobě, podepsané elektronicky.

Lze říci, že zákonem o elektronickém podpisu jsme se přiblížili možnostem, které skýtají dnešní technologie a zejména rozvoj elektronického obchodování. Díky jednoduchosti použití a rozsahu možného využití považují elektronický podpis za přínos pro urychlení a zpřesnění jednání mezi stranami, ať už jde o podnikatelské subjekty či státní instituce. Je třeba samozřejmě dotáhnout použití v rámci veřejné správy do zdárného konce, aby zamýšlený rozsah využití byl i v praxi naplněn.

Mgr. Robert Tschöpl