nou) 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 nějaký podpisový vzor, nezískáváme tím

Možnosti využití digitálních podpisů jsou ohromné: čip na takovéto kartě může obsahovat všechny zobrazené údaje (včetně fotografie v digitální podobě) a jejich digitální podpis, zde vytvořený odpovědnou osobou Policie ČR.

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 věřme, 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*)