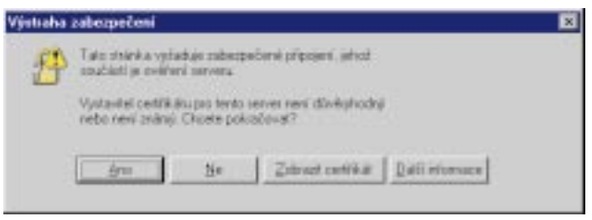
Návrh zákona o elektronickém podpisu

Stihneme informační expres?

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.

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.



Tato výstraha by se po rozšíření digitálních podpisů a certifikačních autorit už nemusela tak často objevovat.

Autory zákona jsou docent Mates a docent Smejkal (posledně jmenovaného znáte za 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

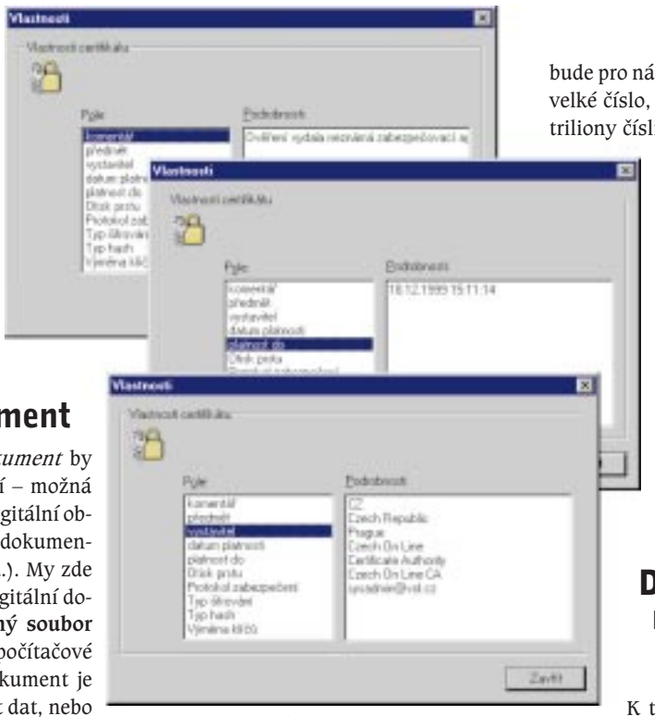
Především je nutno si uvědomit, že **digitální podpis nemá nic společného s pojmy jako zdigitalizovaný podpis nebo naskenovaný podpis**. Digitální podpis je totiž jen a jen **číslo**! Můžeme si je představit jak v desítkové, tak v dvojkové či jiné soustavě. Je to jedno, protože každý z těchto tvarů můžeme 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.



Certifikát v internetové praxi.

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 (taj-