ELEKTRONICKÝ PODPIS

Kateřina Kočková, Lucie Freiwaldová

Zákon č. 227/2002 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

Elektronický podpis není Váš naskenovaný podpis, který si vložíte jako obrázek do textového editoru na konec dokumentu. Jedná se o speciální dokument, který se automaticky připojí k podepisovanému dokumentu a vytvoří tak neoddělitelnou sadu. Z té je možno jednoznačně určit totožnost autora a zjistit, že dokument nebyl po podepsání změněn.

E-podpis tedy vytváří počítač a pro každou odesílanou zprávu je unikátní. Co je tedy potřeba pro to, aby e-podpis mohl vzniknout?

V prvé řadě musí existovat někdo důvěryhodný, kdo ověří vaši totožnost a vydá certifikát, na základě kterého váš počítač generuje pro odesílané zprávy konkrétní e-podpisy. Tím někým důvěryhodným jsou certifikační autority (dále jen CA). Na vás je vybrat si některou CA a u ní si zažádat o vystavení certifikátu. Obvykle lze tuto žádost podat prostřednictvím internetu. Výběr CA záleží na tom, k jakým účelům certifikát potřebujete. Jedná-li se o komunikaci se státní správou, musíte mít certifikát zaručený a ten vydávají pouze některé CA

Kvalifikovaný certifikát tj. 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.

Kvalifikovaný certifikát musí obsahovat :

- označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona o e-podpisu, obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,
- jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,
- zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
- data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
- zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
- číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
- počátek a konec platnosti kvalifikovaného certifikátu,
- případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití, případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

Pokud tedy pomineme oblast komunikace se státní správou, nepotřebujeme certifikát zaručený a zde je již výběr CA podstatně širší. Protože postup získání certifikátu je u každé trochu technologicky jiný, uvedu jako příklad postup u CA Czechia– www.caczechia.cz . Další agentury: AEC, s.r.o. - www.trustport.cz , Globe internet, s.r.o. – www.ca.cz . Ještě před vstupem na stránky na adrese www.caczechia.cz je nutné se rozhodnout, kam

budeme chtít certifikát uložit. Certifikát si totiž nesmíme představovat jako kus krásně potištěného papíru, ale jako datové soubory, tedy něco nehmatatelného. Jedná se o soubory veřejného a osobního klíče. Jak z jejich názvu vyplývá, veřejný klíč slouží ke zveřejnění, a taky k ověření autenticity e-podpisu, osobní klíč musí být naopak velmi pečlivě utajen, protože právě s jeho pomocí vytváří počítač unikátní e-podpis ke každé zprávě. A jsme u jádra problému. Soubory certifikátu jsou sice malé a mohou být uloženy na harddisku počítače. Dokonce jsou chráněny PINem. Pokud je však nemáte zálohovány na nějakém paměťovém médiu (např. disketa či CD-ROM), může se stát, že bude nutno přeinstalovat operační systém počítače a v tom okamžiku o certifikát přijdete. Pokud si zálohu pořídíte, je to potenciální nebezpečí jak může dojít ke kompromitaci osobního klíče. Druhou možností je použít nějaké bezpečné úložiště. Tím může být čipová karta nebo USB token. Tyto prostředky se připojují k počítači a soubory certifikátu z nich nelze žádným způsobem dostat ven. Samozřejmě pojmou i víc certifikátů a lze je použít i k dalšímu zabezpečení počítače. Při použití čipové karty musí být k počítači připojena její čtečka a čipovou kartu lze použít všude tam, kde taková čtečka je. USB token čtečku nepotřebuje, na počítači však musí být nainstalovány jeho ovladače, což je ovšem snadná záležitost.

Pokud se tedy rozhodnete pro použití bezpečného úložiště, je nutné si je nejprve objednat. I to lze provést přímo prostřednictvím www stránek CA Czechia, která nabízí USB tokeny renomovaného světového výrobce. Mít bezpečné úložiště před podáním žádosti o certifikát je nutné proto, že v okamžiku podání této žádosti generuje kryptografický procesor bezpečného úložiště dvojici klíčů (veřejný a osobní). Osobní klíč navíc nikdy bezpečné úložiště neopustí. Pokud bychom bezpečné úložiště v době podání žádosti o certifikát neměli připojeno k počítači, neměli bychom jak vygenerovat potřebnou dvojici klíčů. Tuto dvojici je sice schopen vygenerovat i počítač, ale to by se jednalo o uložení certifikátu do počítače a ne do bezpečného úložiště a to není, jak jsem se již zmínila, právě nejlepší řešení.

Máme-li bezpečné úložiště připojené k počítači, stačí se přihlásit na stránky CA a vyplnit příslušné údaje, kryptografický procesor bezpečného úložiště vygeneruje dvojici klíčů a vše končí vytištěním smlouvy ve dvou exemplářích. Tuto smlouvu sami nepodepisujte!!! Musíte s ní zajít někam, kde mohou ověřit váš podpis (např. notáři, městské úřady apod.) a podepíšete ji až před příslušným úředníkem při ověřování podpisu!!! Potom smlouvu odešlete na adresu CA. Jedna potvrzená kopie se vám vrátí zpět a e-mailem dostanete zprávu odkud a jak si máte nainstalovat vystavený certifikát.

A to je v podstatě vše. Po nainstalování certifikátu kliknete před odesláním e-mailu na ikonu podepsat a po zadání PINu je vygenerován elektronický podpis a zpráva je odeslána. Možná to vypadá složitě, ale zas tak složité to není. Jakmile již máte certifikát vystaven, můžete podepisovat, co hrdlo ráčí.

Využít dnes elektronický podpis můžete pro podání DPH, silniční daně, daně z nemovitosti, zažádat o dávku sociální podpory. Můžete posílat podepsané e-maily na ministerstva. Kompletně komunikovat elektronicky je možné také s některými zdravotními pojišťovnami.

.