Datové schránky pro advokáty – jak na to

II. Pravost elektronického podpisu a jeho exspirace

V minulém díle našeho seriálu jsme se podrobně zabývali otázkou elektronického podpisu (včetně informace kde ho získat a co je pro vás, advokáty, nejpoužitelnější), narazili jsme i na otázku kvalifikovaného časového razítka a jeho použití. Stále nezodpovězenou (a pro advokáty stěžejní) oblastí ovšem zůstává pravost a platnost takového elektronického podpisu. Správné posouzení elektronického podpisu je základním předpokladem pro práci s elektronickými dokumenty. Jak poznat, že podpis, kterým byl podepsán dokument vám doručený, je skutečně pravý a platný?

Protože je dnešní výklad technicky obtížnější, vkládáme něco jako velmi stručné shrnutí celého textu:

1. Přijímat elektronický dokument bez kontroly a pravosti podpisů je velmi riskantní, a to i tehdy, jestliže plně důvěřujete původci dokumentu.
2. Pokud k dokumentu není připojeno kvalifikované časové razítko, přejde dříve či později do stavu, kdy nebude možné ověřit pravost a platnost připojených podpisů.
3. Při použití vhodných softwarových nástrojů jsou veškeré potřebné úkony otázkou několika kliknutí, případně mohou být plně automatizovány.

Kromě toho připomeneme, že **elektronickým podpisem není naskenovaný obrázek ručního podpisu!**

Pokud před sebou máte takový dokument, který současně není opatřen ještě uznávaným elektronickým podpisem, nemůžete takový dokument považovat za platně podepsaný. Takový dokument nelze konvertovat a pracovat s ním jako s originálem – jedná se o pouhou kopii.

Při posuzování pravosti u papírových dokumentů jde o to, zda podpis skutečně vykroužila perem ta osoba, o které se to předpokládá. To znamená, že nepravý podpis nemohl vzniknout jinak než podvodem. U elektronických dokumentů je tomu poněkud jinak. Dokument může být:

a) **Pravý** – to znamená, že lze jednoznačně prokázat, že kontrolní otisk (podpis) nebyl porušen a kterým certifikátem byl kontrolní otisk vytvořen.

b) **Nepravý** – v tom případě není technicky možné ověřit, kdo byl původcem dokumentu. Není to ani v možnostech žádného experta. Dokument je tedy pokládán za nepravý a důkazní břemeno leží na tom, kdo chce jeho pravost prokázat. Není zapotřebí zdůrazňovat, do jak obtížné situace by se držitel dokumentu (případně jeho klient) dostal.

Podstatné je, že **pravý elektronický dokument se může stát nepravým v důsledku nesprávného zacházení, nikoliv zlého úmyslu.**

Kromě toho je teoreticky možné narazit na elektronický dokument, jehož pravost byla narušena tím, že někdo provedl dodatečnou změnu v textu, čímž porušil kontrolní otisk (elektronický podpis). Jednalo by se však o velmi naivní typ podvodu.

Pro advokáta, který přijímá dokument, to znamená, že musí zvládnout dva úkoly:

1. jednoznačně určit, zda jsou všechny podpisy na dokumentu pravé a platné,
2. uložit dokument takovým způsobem, aby pravost i platnost všech podpisů zůstala zachována.

Tyto starosti jsou snad do určité míry kompenzovány tím, že elektronický dokument je daleko odolnější vůči ztrátě, založení do nesprávného šanonu, krádeži, ohni nebo jinému mechanickému poškození i vůči neoprávněnému přístupu. **Stačí dokument nakopírovat do nějakého zabezpečeného úložiště, kde je přístup podmíněn znalostí hesla a kde se automaticky zaznamenává, kdo si dokument prohlížel a kdy.** Takových služeb je na trhu celá řada a jsou vesměs poskytovány za velmi přijatelné ceny.

CRL listina

Než pokročíme k dalšímu výkladu, upozorňujeme, že bez znalosti problematiky vyložené v předchozích dílech seriálu asi nebude srozumitelný. Tento výklad doplníme o nový pojem – **CRL (Certificate Revocation List)**, tedy **seznam odvolaných (revokovaných) certifikátů**.[1] Tento seznam vydává každá kvalifikovaná certifikační autorita.

Seznam CRL je pro posouzení pravosti dokumentu opatřeného elektronickým podpisem důležitý z následujícího důvodu:

Jak jsme uvedli, elektronický podpis je vytvářen pomocí certifikátu, což je malý počítačový program, který má uživatel instalován ve svém počítači nebo na přenosném médiu (token, čipová karta). Jednou ročně je certifikát zneplatněn a jeho majiteli je vystaven nový. Tím je sníženo riziko, že certifikát bude zneužit třeba v důsledku toho, že by jej někdo zapomněl v nepoužívaném notebooku apod. Je ale jistě představitelné, že by mohlo dojít ke zneužití certifikátu například v případě krádeže počítače. Proto je povinností vlastníka certifikátu, aby v případě ztráty kontroly nad svým certifikátem tuto skutečnost oznámil certifikační autoritě, a tím jej zneplatnil. Zneplatnění probíhá tak, že číslo certifikátu je zařazeno na zmíněnou CRL listinu.

1 Dle zákona č. 227/2000 Sb., o elektronickém podpisu, v platném znění.

Kromě toho obsahuje CRL listina čísla certifikátů osob, které zemřely, byly zbaveny svéprávnosti apod.

To znamená, že i zneplatněným certifikátem je možné nadále vytvářet kontrolní otisky (podpisy). Nepravost dokumentu se pozná teprve kontrolou vůči aktuální verzi CRL listiny příslušné certifikační autority.

Seznamy CRL kvalifikovaných certifikačních autorit v České republice najdete na:

První certifikační autorita, a. s.: http://www.ica.cz/Seznamy-zneplatnenych-certifikatu.aspx
Postsignum: http://www.postsignum.cz/seznamy_zneplatnenych_certifikatu_crl.html
eIdentity: http://www.eidentity.cz/ListCRL.html

Manuální kontrola pravosti (platnosti) elektronického podpisu je poměrně komplikovaná, nicméně možná.

K jejímu provedení si **do svého počítače musíte importovat kořenový certifikát příslušné certifikační autority** (postup se liší dle softwarového vybavení, které jste se v souvislosti s otevíráním a prací s PDF dokumenty rozhodli používat) **a kontrolovat aktuální verzi CRL seznamů zneplatněných certifikátů dané certifikační autority**.

Pokud jste ochotni svěřit kontrolu automatu, můžete následující manuál přeskočit.

1. Nejdříve zjistěte, zda je elektronický podpis neporušen. Pokud patříte k té většině, která k prohlížení dokumentů používá Adobe Reader, věnujte pozornost sekci „panel podpisu“ umístěné v pravém horním rohu. Jestliže vám po kliknutí na tento panel počítač ukáže hlášku „Dokument se od aplikování tohoto podpisu nezměnil“, je vše v pořádku. V opačném případě je na místě dokument odmítnout. Otazníku, který bude prohlížeč ukazovat, si v této chvíli nemusíte všímat.

2. Zjistěte, která certifikační autorita vydala certifikát, který byl použit při podpisu. Kromě tří zmíněných kvalifikovaných certifikačních autorit se může jednat o kvalifikovanou certifikační autoritu z jiného státu EU (pak je vše v pořádku – certifikáty všech kvalifikovaných autorit v zemích EU jsou uznávány ve všech státech EU) nebo o certifikační autoritu, která není kvalifikovaná, a platnost podpisu je tudíž v nejlepším případě velmi problematická.

3. Teď přichází krok, ve kterém je třeba importovat kořenový certifikát příslušné certifikační autority do počítače a současně správně nastavit prohlížeč PDF dokumentů, který jste se rozhodli používat. Podrobný návod najdete na stránkách výrobce prohlížeče nebo certifikační autority. Dobrá zpráva je, že **kořenový certifikát každé certifikační autority instalujete pouze jednou.**

4. Znovu se podívejte do panelu podpisu. V ideálním případě se ujistíte, že certifikát byl skutečně vydán touto certifikační autoritou a že jeho platnost dosud nevypršela.

5. Podíváte se na aktuální CRL příslušné certifikační autority a zkontrolujete, zda v ní není uvedeno číslo příslušného certifikátu.

6. Pokud podpis obstál v kontrole předchozích dvou bodů, máte před sebou pravý a platný dokument. Připomínáme jen, že **pokud je k dokumentu připojeno několik podpisů, má být kontrola provedena s každým podpisem samostatně**.

7. Pokud se při kontrole ukázalo, že platnost certifikátu již vypršela nebo certifikát byl zařazen na CRL listinu, musíte zjistit, jak to bylo s platností certifikátu v době, kdy byl podpis připojován. K tomu potřebujete, aby k dokumentu bylo připojeno také kvalifikované časové razítko. Pokud kvalifikované časové razítko k dokumentu připojeno není, dokument v žádném případě nepřijímejte. Jeho pravost a platnost není možné ověřit.

Pokud jste některé z předcházejících řádek vynechali, nedivíme se vám. Ve skutečnosti i jen málokterý IT specialista je schopen vše bez problémů zvládnout.

Schůdnější cestou je pořízení nějakého technického nástroje, který tuto kontrolu provede za vás, příliš vás nezatíží a bude uživatelsky jednoduchý. Na světě je takových nástrojů několik, v České republice zatím pouze služba **SecuStamp.com**, o které jsme se zmínili v minulém díle. Funguje tak, že posuzovaný dokument vložíte do internetového rozhraní a během několik vteřin dostanete posudek, případně ověřovací doložku. Posudek je zdarma, ověřovací doložka k jednomu dokumentu vyjde řádově na korunu. Více informací získáte na: http://www.secustamp.com/.

Pro získání plné jistoty je dobré provést ověření až 12 hodin poté, co dokument obdržíte. To je doba potřebná k tomu, aby se případné zneplatnění certifikátu promítlo do aktuální verze CRL. Ostatně i posudek vydaný dříve než 12 hodin po podpisu potvrdí pravost s výhradou.

Ověření tedy proběhlo. Pokud dokument testem neprošel, neznamená to nutně, že byste byli obětí podvodu. Původce možná jen zanedbal technickou stránku věci nebo prostě nemá dostatečné znalosti. V tom případě je na místě dokument odmítnout a požádat protistranu, aby vyhotovila korektní verzi. Pokud se jedná o archivní dokument, který není možné znovu podepsat, máte smůlu. Originál vám rozežraly elektronické myši a existuje již jen kopie.

Pokud dokument testem prošel, potřebujete zajistit, že si pravost a platnost udrží. Jak již bylo uvedeno, platnost použitého certifikátu dříve či později vyprší nebo bude revokována (odvolána). Stane se tak nejpozději za 12 měsíců, ale možná již za několik hodin. Pokud by k tomu došlo, dokument se stane neověřitelným a nebude již existovat žádná možnost, jak jej opravit.

Proto je důležité zkontrolovat nejen momentální pravost a platnost, ale také

1. jestli je k dokumentu připojeno rovněž kvalifikované časové razítko,
2. jestli toto časové razítko bylo připojeno zároveň s posledním podpisem nebo později.

(Při zmíněném ověření pravosti a platnosti podpisů se dozvíte obojí.)

Zjistíte-li, že dokument tyto požadavky nesplňuje, neztrácejte ani minutu a časové razítko připojte (získáním a připojením kvalifikovaného časového razítka jsme se podrobně zabývali v předcházejícím díle). Teď už jen stačí dokument uložit (nejlépe do nějakého zabezpečeného úložiště).

Máte otázky k datovým schránkám? Neváhejte se na nás obrátit! Pište své dotazy na e-mail datoveschranky@cak.cz. Na dotazy budeme odpovídat, nejčastější dotazy a odpovědi na ně budou umístěny na úvodní stránce webu ČAK pod banner „Datové schránky a advokáti – jak na to“. Zde postupně najdete také všechny informace, které budeme publikovat v tomto seriálu k datovým schránkám.

✤ odbor vnějších vztahů ČAK