Datové schránky pro advokáty – jak na to

I. Před prvním přihlášením do datové schránky – aneb co všechno budu potřebovat a kde to získám

Dříve, než se poprvé přihlásíte do datové schránky, zkontrolujte, zda váš počítač a jeho softwarové vybavení odpovídá požadavkům.[1] Česká pošta uvádí, že stačí jakýkoliv běžný osobní počítač nebo notebook s připojením k internetu, je ovšem zapotřebí rozumět, co se v tomto případě „běžným osobním počítačem" myslí.

Technické a programové vybavení

1. Prvním předpokladem je tedy **vlastnit pevný stolní počítač nebo notebook** s operačním systémem Microsoft Windows 7, Vista nebo XP (tedy koupený v roce 2005 nebo později). Do datové schránky můžete přistupovat i z počítačů Mac nebo počítačů s operačním systémem Linux, v přípravě je i verze pro tablety. To je však speciální problematika, kterou se nebudeme zabývat.

2. Počítač musí být připojený k internetu. Doporučovaná rychlost 128kb/s znamená, že stačí opravdu jakékoliv připojení.

3. Co se týče programů, potřebujete **internetový prohlížeč** (jakýkoliv, například Internet Explorer, Mozzila Firefox nebo Google Chrome), **prohlížeč PDF dokumentů** (nejčastěji Adobe Acrobat Reader) a **formulářový prohlížeč** Software602 Form Filler.

Internetový prohlížeč máte ve svém počítači zcela jistě, další dva zmíněné programy musíte nainstalovat (pokud je dosud nemáte). Instalace je velmi jednoduchá. Otevřete příslušnou internetovou stránku

http://www.602.cz/602xml_filler/download a

http://www.slunecnice.cz/sw/acrobat-reader/

či http://get.adobe.com/reader/otherversions/ (zadejte operační systém a jazyk), klikněte na „stáhnout", a poté několikrát na „ano" nebo „pokračuj".

4. Takto vybavený počítač vám umožní přijmout datovou zprávu, korektně ji uložit, otevřít přiložený dokument (například rozhodnutí) a tento dokument samostatně uložit. **Pokud chcete datové zprávy nejen přijímat, ale i odesílat, potřebujete nástroj, kterým vám umožní vytvořit dokument ve formátu PDF a podepsat jej elektronickým podpisem.** Takových nástrojů existuje celá řada.

Nejběžnějším produktem je software **Adobe Acrobat** (Pozor! Nezaměňovat s výše zmíněným Adobe Acrobat Reader!), jehož asi jedinou nevýhodou je cena cca 9000 Kč (bez DPH) na jeden počítač. Pokud se pro něj rozhodnete, získáte ovšem zároveň profesionální grafický nástroj. Bližší informace najdete u českých distributorů, například www.amsoft.cz, více informací můžete nalézt zde: http://www.adobe.com/cz/purchase/.

V České republice je často používanou alternativou produkt firmy Software602 **Print2PDF**, který je v jednouživatelské verzi ke stažení zdarma. Co se šíře funkcí týká, nemůže s produktem Adobe Acrobat soutěžit, to je však vyváženo jednoduchostí. Umožní vám provést základní úkony, jako spojení několika dokumentů a tabulek do jednoho PDF, převod do archivačního PDF/A, překrytí souboru vodotiskem, zabezpečení heslem, zadání ochrany proti kopírování obsahu – a pochopitelně také připojení elektronického podpisu. Stáhnout si jej můžete na http://www.602.cz/print2pdf/.

Kromě toho existuje řada nástrojů, které slouží buď k převodu běžného textu do PDF (například **PDF Creator**) nebo k připojení podpisu (například **PDF Signer** firmy Dignita s. r. o., http://www.maxiorel.cz/pdf-signer-elektronicky-podpis-pdf-dokumentu či http://www.recomando.cz/programy-pro-elektronicky-podpis) a které jsou rovněž k dispozici zdarma. Jestli máte dost času a nevyžadujete, aby program fungoval v češtině, můžete jich na internetu najít stovky.

Pokud v tuto chvíli přemýšlíte o tom, že zprávy budete pouze přijímat, ale odesílat nechcete, neboť to s sebou přináší jen problémy (a přece funguje ještě pošta, máte již nastaveny procesy ve vaší kanceláři a převažuje nechuť se pouštět do něčeho nového), upozorňujeme, že situace kolem datových schránek pomalu a jistě spěje do bodu, kdy budou muset přijímat a odesílat všechny subjekty povinně. V celkovém objemu nových informací, práce a vynaložených financí už není tento krok tak dramatický a rozhodně doporučujeme vydat se cestou komplexního využívání datových schránek – tedy přijímat i odesílat datové zprávy!

1 Tento seriál je primárně určen pro ty advokáty, kteří se rozhodnou do datové schránky přistupovat přes webové rozhraní. Pro advokáty, kteří mají zájem přistupovat do datové schránky přes specializované produkty různých firem, je na trhu dnes již velké množství možností. Pokusíme se uvést některé z nich, výčet ovšem rozhodně nebude vyčerpávající. Tyto produkty a jejich popis nejsou předmětem tohoto seriálu.

Elektronický podpis

Dokument (ve formátu PDF), který chcete datovou schránkou odeslat, musíte podepsat (neboli připojit k němu) **uznávaný elektronický podpis**. K tomu potřebujete **kvalifikovaný certifikát**. Certifikát můžeme přirovnat k pečetidlu, které zůstává pod kontrolou vlastníka, ale je možné rozpoznat jeho otisk na jednotlivých listinách.

O vydání kvalifikovaného certifikátu musíte požádat akreditovanou certifikační autoritu. V současné době působí v České republice tři akreditované certifikační autority:

První certifikační autorita, a.s. – http://www.ica.cz/
PostSignum – http://www.postsignum.cz/
eIdentity – http://www.eidentity.cz/

Orgány veřejné moci jsou ze zákona povinny uznávat i elektronické podpisy vytvořené pomocí kvalifikovaných certifikátů vydaných akreditovanými certifikačními autoritami ve všech zemích EU. Takových certifikačních autorit je přibližně 70. To znamená, že pokud chcete, můžete si nechat vytvořit certifikát i v zahraničí. Tím se však náš seriál zabývat nebude.

Připomeňme si, co je elektronický podpis a certifikát:

Elektronický podpis – jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. Tolik legislativa. Převedeno do počítačové technologie to znamená, že k dokumentu je neoddělitelně připojen jeho kontrolní otisk. Počítač příjemce je schopen provést kontrolu, zda otisk odpovídá dokumentu a tudíž zda v dokumentu nebyly provedeny dodatečné změny (jak si ukážeme později, k takové kontrole stačí jediné kliknutí a porozumění těm nejzákladnějším principům).

Elektronický podpis zabezpečuje dokument z klíčových hledisek informační bezpečnosti:

INTEGRITA. Příjemce dokumentu má jistotu, že jej dostává přesně v tom znění a v tom stavu, v jakém jej původce vytvořil. I ta nejmenší změna se projeví „rozbitím podpisu“ (dokument a jeho kontrolní otisk již do sebe nezapadají) a jednou rozbitý podpis není možné žádným způsobem opravit.

NEPOPIRATELNOST. Ten, kdo použil svůj certifikát k vytvoření podpisu (kontrolního součtu), nemůže zpochybnit, že je původcem dokumentu. Z toho vyplývá, že **bude-li váš certifikát odcizen, může pachatel provádět vaším jménem právní úkony**. Pokyny, jak postupovat v případě podezření na odcizení certifikátu, uvedeme později.

AUTENTICITA. Není technicky možné, aby se jiná osoba úspěšně vydávala za vlastníka certifikátu. Pokud se čtenář nespokojí s tímto konstatováním, doporučujeme, aby si v nějaké technické publikaci prostudoval témata „PKI“ a „asymetrické šifrování“.

Jak vyplývá z výše uvedeného,

1. elektronický podpis není obrázkem ručního podpisu.

2. elektronický podpis nemůže být připojen na konkrétní místo v dokumentu. **Jedná se o otisk celého dokumentu.**

Certifikát je počítačový program, jehož pomocí se vytvářejí kontrolní otisky dokumentů. Pro naše účely je podstatné rozumět tomu, že:

- Z elektronického podpisu (kontrolního otisku) je vždy možné jednoznačně a nepopiratelně určit, kterým certifikátem byl vytvořen.
- Není technicky možné, aby elektronický podpis byl padělán. Bez prolomení šifry totiž není možné napodobit otisk vytvořený cizím certifikátem (to je vlastností výše zmíněného asymetrického šifrování).
- Nic nebrání tomu, aby kdokoliv vyráběl certifikáty a rozdával je svým zaměstnancům, přátelům, členům klubu apod., kteří je budou používat k vytváření kontrolních otisků/podpisů. Orgány veřejné moci ale takové podpisy pochopitelně neuznávají.

Certifikační autoritou můžeme rozumět zařízení, které certifikáty vytváří, a zároveň organizaci, která se touto činností zabývá. Pro naše účely jsou důležité akreditované certifikační autority, které jsou schopny u každého certifikátu doložit totožnost osoby, které byl certifikát vydán, a to takovým způsobem, že je to hodnověrné pro veřejnou správu.

I certifikační autorita vám může vydat dva různé druhy certifikátů:

Kvalifikovaný certifikát pro vytváření uznávaného elektronického podpisu – potřebujete ke komunikaci s veřejnou správou.

Komerční certifikát je určený pro bezpečné přihlašování do různých systémů včetně Czech POINTu a systému datových schránek (tedy něco jako elektronický důkaz vaší totožnosti).

Podle našich zkušeností je výhodné pořídit si hned na začátku oba zmíněné certifikáty a nechat si je umístit na USB klíčenku (token) nebo čipovou kartu.

Je to bezpečnější a vyhnete se technickým komplikacím. Zabezpečenou klíčenku nebo čipovou kartu vám prodá přímo certifikační autorita (je též možné využít nový identifikační průkaz advokáta). Je ovšem dobré předem zkontrolovat, zda má váš počítač čtečku čipových karet či si tuto čtečku pořídit.

1. Pokud využijete čipové karty od certifikační autority, měla by vám taková certifikační autorita být schopna nabídnout i čtečku čipových karet, která bude vhodná pro ten který druh karty. Zeptejte se na tuto možnost.

2. Pokud chcete využít nový identifikační průkaz advokáta jako bezpečné úložiště certifikátů, doporučujeme využít tyto čtečky: Omnikey Cardman 5321 (nebo Omnikey Cardman 5321CL), stolní varianty Omnikey Cardman 3121 či 3021 (objednat můžete například zde: http://www.sovte.cz/ctecky/cenik_ctecky_cipovych_karet.php).

Dobře vám poslouží ale i většina běžně používaných čteček (např. ty, které poskytuje banka, příkladem námi vyzkoušené čtečky, která funguje, je GemPC Twin).

Důležité je ovšem mít nainstalovány ovladače k takové čtečce – získáte je na webu ČAK: http://podpora.cak.cz/prukazy/. **V případě technických problémů neváhejte využít linky technické podpory, tel.: 226 806 406.**

Důležité upozornění – certifikáty vám budou vydány na základě vaší osobní návštěvy u některé z certifikačních autorit, je třeba mít s sebou dva doklady totožnosti, nelze tedy vyslat jako zástupce sekretářku či získat certifikát přes internet![2]

Platnost certifikátu je u všech certifikačních autorit stejná – jeden rok. Po roce vám certifikační autorita automaticky vytvoří nový certifikát (a pošle fakturu).

Jak se ale vyznat v nabídce certifikačních autorit a zažádat o ten správný produkt?

První certifikační autorita, a.s. – tato autorita nabízí produkt, který se nazývá **TWINS**. Produkt obsahuje kvalifikovaný a komerční certifikát na bezpečném úložišti – token nebo čipová karta. Můžete bez obav využít token či čipovou kartu Starcos, které vám tato certifikační autorita nabídne. **Můžete ovšem také jako bezpečné úložiště využít váš nový identifikační průkaz advokáta!** Není tedy třeba pořizovat novou čipovou kartu jen na certifikáty, ale váš průkaz se tímto může stát víceúčelovým.

PostSignum – neboli certifikační autorita České pošty – tato certifikační autorita nabízí produkt, který se nazývá **Bezpečný přístup k datové schránce (KOMPLET)**. Tento produkt obsahuje všechny tři komponenty, které potřebujete – kvalifikovaný certifikát, komerční certifikát a token. K dnešnímu dni nemáme zprávu o tom, že by tato certifikační autorita nevydávala certifikáty i na identifikační průkaz advokáta – máte-li zájem o služby této certifikační autority, určitě využijte i této možnosti.

eIdentity – vhodným produktem pro vás, advokáty, je u této certifikační autority **Balíček kvalifikovaného certifikátu a k němu vydaného komerčního certifikátu.**

Existují dvě cesty, jak certifikáty (uložené na identifikačním průkazu advokáta) získat:

1. Kontaktujte certifikační autoritu a navštivte výdejní místo dle vašeho bydliště (kontakty naleznete na stránce http://www.ica.cz – pravý strom – Registrační autority – zadejte kraj).

2. Chcete na výdejním místě strávit co nejméně času? Vygenerujte si žádost již doma na svém osobním počítači. K tomu vám poslouží speciální URL adresa (kterou vám na požádání sdělí na lince technické podpory ČAK – podpora@podpora.cak.cz, tel.: 226 806 406). Postup je potom následující:

2 Jiná situace je ovšem při prodlužování certifikátu – toto prodloužení je již možné udělat bez vaší osobní návštěvy a potřebujete k tomu jen připojení na internet.

- Na URL adrese je možné vygenerovat žádost o oba certifikáty (kvalifikovaný i komerční) v jednom kroku a uložit ji na čipovou kartu advokáta (identifikační průkaz advokáta) postupem uvedeným v příloze pro Internet Explorer (doporučení: zkopírovat odkaz do prohlížeče, nikoli jen kliknout).
- Tento postup je možný na PC/noteboocích pro operační systémy od Windows Vista výše (včetně WIN7).
- Dostavte se s žádostí na čipové kartě na veřejnou registrační autoritu dle vašeho bydliště (viz www.ica.cz – pravý strom – Registrační autority – zadejte kraj) a požádejte o vydání certifikátů na čipovou kartu.

Kvalifikované časové razítko

Posíláte-li nějaké pdf přes datovou schránku a má-li tento dokument zásadní povahu (tj. předpokládáte delší životnost než jeden rok, nejedná se tedy o dokument krátkodobé povahy jako je například pozvánka), měli byste kromě uznávaného elektronického podpisu dokument opatřit i **kvalifikovaným časovým razítkem.**

Rozumíme-li, co je elektronický podpis a k čemu je dobrý, je důležité porozumět tomu, co je časové razítko.

Představme si advokáta, který v zastoupení svého klienta obdržel elektronický dokument opatřený uznávaným elektronickým podpisem protistrany. Provede kontrolu platnosti podpisu (jak se taková kontrola provádí, vysvětlíme později) a uloží dokument ve svém počítači. Pro jistotu jej také zkopíruje na nějaké externí paměťové zařízení, které umístí v trezoru. Pokud se cítí bezpečně, je na omylu.

Stačí, aby protistrana zatelefonovala do certifikační autority a nechala zneplatnit certifikát, kterým byl podpis (kontrolní otisk) vytvořen. Náš advokát nemá v zásadě žádnou možnost se o této nové skutečnosti dozvědět (jedinou možností je každý den kontrolovat seznamy zneplatněných certifikátů).

Po nějaké době je advokát vyzván k předložení dokumentu. Předloží jej tedy rozhodčí instanci a ta provede kontrolu

platnosti podpisu s následujícím výsledkem: Podpisový certifikát není platný a není tudíž možné rozhodnout o pravosti dokumentu. To, co má advokát v počítači i trezoru, náhle není nic jiného než neověřená kopie.

Nemusí se přitom vždy jednat o zlý úmysl původce dokumentu. Certifikáty se vystavují s dvanáctiměsíční platností. To znamená, že každých 12 měsíců jsou zpochybněny všechny podpisy, které byly během uplynulého roku vytvořeny. V tomto případě nepomůže ani prodloužení platnosti certifikátu – toto prodloužení si představme jako vygenerování nového certifikátu (s novým číslem), ale už bez nutnosti prokazování své totožnosti u certifikační autority.

Nabízí se přirozená námitka, že v době, kdy byl dokument předán, byl ještě platný. V dokumentu je skutečně uvedeno datum a čas připojení podpisu (a dá se velice snadno zjistit, že ke zneplatnění certifikátu došlo později). Jedná se však o datum a čas odvozené z počítače uživatele, a tudíž neprůkazné.

Z toho vyplývá, že připojení uznávaného elektronického podpisu k dokumentu nemusí stačit. Spolu s podpisem by mělo být připojeno také kvalifikované časové razítko, a to **proto, že připojením kvalifikovaného časového razítka zajistíte DLOUHODOBOU právní váhu dokumentu.**

I časové razítko je kontrolním otiskem dokumentu. Z časového razítka ovšem nevyčtete, kdo jej vytvořil, ale kdy bylo vytvořeno. Čas potom není (a ani nemůže být) odvozen od času ve vašem počítači, ale od hodin v centrále kvalifikované certifikační autority. Vzniká tak nezpochybnitelný důkaz, že dokument existoval v určitém časovém okamžiku a jak v tu danou chvíli vypadal.

Pro advokáty z toho vyplývají dva praktické důsledky:

1. Je naivní a nezodpovědné archivovat elektronické dokumenty, ke kterým je připojen elektronický podpis, ale chybí časové razítko (důležité je, že razítko musí být připojeno později než podpis). Advokát by měl provést kontrolu dokumentu, a pokud časové razítko chybí, buď ho připojit, nebo dokument konvertovat do listinné podoby.

Pokud dokument prošel datovou schránkou, je časové razítko připojeno na „obálce“. Tím je situace usnadněna, případné prokazování by však bylo technicky poměrně komplikované.

Stanovisko Ministerstva vnitra z 6. dubna 2010 ukládá orgánům veřejné moci, aby časové razítko připojovaly ke všem dokumentům vkládaným do datové schránky. Opírá se přitom o výklad zákona č. 499/2004 Sb. o archivnictví a spisové službě a změně některých zákonů. V praxi ovšem můžete narazit na úřady, které tuto povinnost ignorují. Je tedy důležité kontrolovat, zda je opravdu připojeno.

2. Pokud vytváříte dokument zásadní povahy a odesíláte jej datovou schránkou, měli byste kromě uznávaného elektronického podpisu opatřit dokument také kvalifikovaným časovým razítkem.

Už samotný název napovídá, kam se obrátit a kde hledat dodavatele služby připojování časových razítek – je to opět akreditovaná (kvalifikovaná) certifikační autorita. První věc, která vás při pořizování této služby překvapí, je její cena – platíte za připojení každého jednotlivého časového razítka. Nicméně bez časového razítka se neobejdete, takže nezbývá, než zaplatit.

Chcete-li získat možnost opatřovat své dokumenty časovým razítkem, máte v současné chvíli dvě možnosti:

1. Oslovit certifikační autoritu a získat tuto možnost přímo od ní. Tato možnost je výhodná pro velké advokátní kanceláře, které jsou schopny a ochotny investovat do technického vybavení své kanceláře a dokáží dobře odhadnout, kolik časových razítek za dané období spotřebují (cena se totiž odvíjí od toho, kolik časových razítek si za dané období pořídíte, čím více, tím příznivější cena).

2. Na trhu již existují i možnosti pro malé kanceláře či samostatné advokáty. Jsou to produkty, které vás nezavazují podepisovat smlouvy či řešit otázku propojení s certifikační autoritou. Kupujete balík razítek a postupně tento balík spotřebováváte – nejste tedy časově omezeni, záleží jen na vás, za jak dlouho tento balík spotřebujete. Tuto službu nabízí například firma Software602 s produktem **SecuStamp.com** (více na http://www.secustamp.com/, zde si můžete stáhnout i demo verzi 25 časových razítek zdarma). Tato služba slouží i k ověření platnosti elektronických podpisů, kterému se budeme věnovat v dalších částech našeho seriálu.

Není toho zrovna málo, že? Nebojte se, dá se to zvládnout! Postupujte krok po kroku a nechtějte mít všechno vyřešeno během jednoho dne (to není v silách nikoho). Máte-li ve svém okolí nějakého technicky zdatného poradce, neváhejte se na něj obrátit. Nevíte-li si rady s certifikáty, nebojte se kontaktovat linky technické podpory té které certifikační autority.

S dalšími technickými problémy se můžete obracet na linku technické podpory ČAK (tel.: 226 806 406).

Po novém roce pro vás chystáme instruktážní film, kde si krok po kroku názorně ukážeme, jak postupovat. Do konce roku by pro vás měl být připraven i intuitivní průvodce kartou (novým identifikačním průkazem), pomocí kterého si sami vygenerujete žádost o certifikát.

Sledujte dál informace v tomto seriálu a na webových stránkách ČAK.

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