Jiří Peterka

Báječný svět elektronického podpisu

Edice CZ.NIC

Jiří Peterka
BÁJEČNÝ SVĚT ELEKTRONICKÉHO PODPISU

www.bajecnysvet.cz

Vydavatel:
CZ.NIC, z. s. p. o.
Americká 23, 120 00 Praha 2
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2011
Kniha vyšla jako 4. publikace v Edici CZ.NIC.
ISBN 978-80-904248-3-8

ISBN 978-80-904248-3-8

— Jiří Peterka

Báječný svět elektronického podpisu

— Edice CZ.NIC

Předmluva

Vážení čtenáři,

když jsme před rokem a půl s Edicí CZ.NIC začínali, měli jsme trochu obavy, zdali bude dostatek českých autorů, kteří budou schopni napsat knihy, které by svým charakterem zapadaly do náplně naší edice.

Ačkoliv se od spuštění edice snažíme aktivně přemlouvat některé české osobnosti k napsání vlastního díla, po úvodní knize Pavla Satrapy jsme skutečně museli dvakrát sáhnout do zahraničí. Nicméně nakonec se to podařilo a na naši nabídku kývla osobnost, kterou osobně považuji za osobnost s velkým O, vysokoškolský pedagog, publicista a odborný konzultant RNDr. Jiří Peterka.

Představovat přínos pana Peterky pro oblast elektronického podpisu v této zemi je poměrně zbytečné. Při zkoumání jeho elektronického archivu na adrese **www.earchiv.cz** jsem napočítal více než 40 různých článků na toto téma, které vyšly v posledních jedenácti letech v novinách a časopisech. Těžko bychom tedy hledali osobu povolanější pro sepsání takovéto knihy.

Přiblížit laikům složitou oblast elektronického podpisu včetně jejích kryptografických aspektů se může jevit jako obtížný úkol. Nicméně od samého začátku, a vzhledem i k mé vlastní zkušenosti, jsem si byl jist, že v tomto se plně projeví fakt, že pan Peterka není jen odborníkem ale také pedagogem.

A výsledek mě v tomto skutečně nezklamal. Kniha je čtivá i pro laika s minimem znalostí o dané problematice, který se tak může velmi pozvolným a přirozeným způsobem do problematiky ponořit. Přesto je ale nabitá velmi zajímavými informacemi a postřehy, které překvapí a potěší i znalce.

Ještě mi dovolte zmínit jednu novinku tohoto vydání. Od samého začátku jsme vydávali každou knihu „dvojmo“, tedy v papírové podobě a také v elektronické verzi ve formě volně stáhnutelného PDF souboru. Tuto knihu budete moci číst ještě na jiném médiu a to na čtečkách elektronických knih.

Ať už tedy držíte v ruce knihu, čtečku či počítač, nechť se Vám kniha pana Peterky líbí.

Ondřej Filip
V Praze 3. dubna 2011

Předmluva autora a ediční poznámka

Vydavatelská a autorská verze knihy

Tato kniha vychází v Edici CZ.NIC ve dvou verzích: vydavatelské a autorské. Obě jsou obsahově shodné, ale liší se sazbou a některými dalšími vlastnostmi (například pokud jde o používání hypertextových odkazů či možnost změny).

Vydavatelská verze je optimalizována pro klasický knižní tisk, je pouze černobílá a je vysázena podle konvencí Edice CZ.NIC (pro rozměry tištěných titulů, vydávaných v této edici). Je dostupná v tištěné podobě, ale je možné ji získat i v podobě elektronické (ve formátu PDF, který je přesnou kopií tištěné podoby).

Autorská verze je naproti tomu optimalizována pro používání v elektronické podobě a nebude vydávána v tištěné podobě. Je formátována přímo autorem a skrze aktivní hypertextové odkazy je propojena i s on-line podporu knihy na webu, která nabízí mj. příklady podepsaných elektronických dokumentů či obrázky v plné velikosti (stačí kliknout na odkaz v legendě ke konkrétnímu obrázku). Autorská verze je dostupná jak ve formátu PDF (vysázená pro stránky A4), tak ve formátech pro elektronické čtečky.

Díky své čistě elektronické podobě se autorská verze může měnit, s tím jak budou opravovány případné chyby či jak bude třeba reagovat na změny v oblasti elektronického podpisu (například na nové poznatky, služby, produkty či změny v legislativě). Proto jsou jednotlivá vydání autorské verze číslována (od 1.00).

Všechny elektronické verze (autorská i vydavatelská) jsou dostupné ke stažení z webu Edice CZ.NIC. Zde je také možné objednat tištěnou podobu (vydavatelské verze) knihy. On-line podporu knihy je možné nalézt na adrese **http://bajecnysvet.cz.**

Předmluva autora

Elektronický podpis je zajímavým fenoménem naší současnosti. Mnoho lidí jej již používá a ještě více by jej rádo používalo. Stát dokonce v mnoha situacích jeho užití nařizuje a vymáhá, zejména v souvislosti s celkovou elektronizací veřejné správy a jejích agend.

Již méně se ale pamatuje na to, že práce s elektronickými podpisy je přeci jen zásadně jiná, než práce s vlastnoručními podpisy. Může být srovnatelně jednoduchá a může dokonce přinášet mnohonásobně vyšší míru spolehlivosti, než podpisy vlastnoruční. Na druhé straně se opírá o zcela jiné principy, vyžaduje zcela odlišné postupy a může mít také dosti odlišné souvislosti a dopady, než práce s vlastnoručními podpisy na listinných dokumentech.

Znalost těchto principů, postupů i souvislostí a dopadů elektronického podpisu je ale často podceňována. Někdy dokonce i záměrně ignorována, a to aktivním prosazováním představ o tom, že „s elektronickými podpisy je to vlastně stejné, jako s vlastnoručními podpisy“. To opravdu není.

Hlavní motivací pro vznik této knihy bylo přispět k tolik potřebné osvětě kolem elektronického podpisu. A to formou srozumitelnou i pro lidi, kteří nejsou a nepotřebují být odborníky v kryptografii ani počítačovými specialisty. Formou, která by je uvedla do báječného světa elektronického podpisu, a současně je neodradila přílišnou složitostí a záplavou detailů. Formou, která by je inspirovala k přemýšlení nad realitou tohoto báječného světa a motivovala k jeho dalšímu poznávání.

Snaha napsat takovouto knihu ale přinesla nejedno velké dilema. Třeba nutnost nahradit celé rozsáhlé a velmi technické pasáže – jako například samotnou podstatu asymetrické kryptografie – něčím, co by bylo stručné, jasné a srozumitelné i tomu, kdo nemá žádné předchozí znalosti. Zde jsem si pomohl přirovnáním k bezpečnostním schránkám se dvěma dvířky, či představou „kafemlýnku“, který na požádání „semele“ různé ingredience. Laik doufejme pochopí a odborník snad promine.

Nejtěžším úkolem ale bylo zvládnutí obrovské šíře celé problematiky, včetně terminologie a všech souvislostí. Jak popisovat vše postupně, aby to nebylo jen samé odkazování na další a další kapitoly, kde teprve bude vše vysvětleno? Jak neodradit čtenáře hned na začátku celou záplavou detailů a jak mu pomoci, aby se v celé problematice neztratil?

Nakonec jsem zvolil „tříúrovňovou" koncepci: celá problematika elektronického podpisu je v této knize popisována na třech různých úrovních, které se částečně překrývají. Na nejvyšší úrovni (v první kapitole) jsou základní pojmy a souvislosti elektronického podpisu podány jakoby nanečisto, více zjednodušenou a také mnohem kratší formou tak, aby čtenář získal určitý celkový přehled. Aby věděl a tušil, co bude následovat na druhé úrovni (ve druhé, třetí a čtvrté kapitole) při přeci jen detailnějším výkladu a popisu principů elektronického podpisu. Na třetí úrovni (v páté až osmé kapitole) pak jsou řešeny praktické aspekty práce s elektronickým podpisem: příprava počítače (s MS Windows), podepisování PDF dokumentů, podpora elektronických podpisů v kancelářském balíku MS Office a, v neposlední řadě, i „související" oblasti jako je šifrování, přihlašování či zabezpečená komunikace.

Rád bych touto cestou poděkoval všem, kteří mi pomohli s přípravou knihy. Zejména (v abecedním pořadí dle příjmení): Jaroslavu Kučerovi z Krajského soudu v Liberci, Miroslavu Novákovi ze společnosti ARCDATA Praha, Janu Podanému z Okresního soudu v Kladně, Vladimíru Sudzinovi z Ministerstva vnitra ČR, Jaroslavu Tománkovi a Lucii Urbanové ze společnosti I. CA, Pavlu Vondruškovi ze společnosti Telefónica O_2 Czech Republic.

Jiří Peterka
V Praze, 2. dubna 2011

Obsah

Přehled kapitol

Úroveň I – Přehled

Kapitola 1

Úroveň II – Principy

Kapitola 2

Kapitola 3

Úroveň I – Přehled

1. Základní pojmy a souvislosti

Kapitola 1

1. Základní pojmy a souvislosti

V oblasti elektronického podpisu, stejně jako snad ve všech oblastech lidské činnosti, se používá specifická terminologie. I zde se tedy setkáme s termíny, které jinde vůbec nenajdeme, nebo které mohou jinde mít i poněkud odlišný význam. Přesné vysvětlení většiny těchto pojmů ale není možné bez toho, abychom znali řadu souvislostí a hlavně principů, o které se fungování elektronického podpisu opírá.

Pojďme si tedy, v souladu s „tříúrovňovým" charakterem výkladu v této knize, potřebné základní pojmy a souvislosti nejprve alespoň nastínit, zatím bez nějakého detailnějšího (a hlavně přesnějšího) vysvětlování. Pokud to bude vhodné, zkusíme si naznačit jejich podstatu alespoň intuitivně a neformálně, tak abychom ji v dalším textu mohli postupně upřesňovat.

No a tam, kde příslušný pojem může mít nějaké grafické znázornění, si ho zkusíme ukázat hned, i když třeba ještě nedoceníme všechny detaily.

1.1 Zpráva vs. dokument

Ze všeho nejdříve se domluvme na jedné důležité konvenci, která se týká volby mezi pojmy **dokument** a **(datová) zpráva**. V oblasti elektronického podpisu se totiž používají oba tyto termíny. Někdy se tak hovoří o (elektronickém) podepisování zpráv, jindy o (elektronickém) podepisování dokumentů. Obecně mezi dokumentem a (datovou) zprávou nemusí být rozdíl. V praxi ale mnohdy bývá. Například u datových schránek je zcela zásadní rozdíl mezi datovou zprávou a dokumentem, obsaženým v datové zprávě.

I mimo oblast datových schránek ale může být rozdíl v tom, že pojem „zpráva" evokuje představu přenosu (odněkud někam), zatímco pojem „dokument" takovouto představu nevnucuje (dokument můžeme uchovávat stále na jednom místě). Od zprávy také obvykle nepožadujeme nějakou delší životnost (potřebujeme ji pouze pro jednorázový přenos), zatímco od dokumentu ano. Mnohdy chceme a potřebujeme mít možnost pracovat s dokumentem třeba i po desítky let.

Proto v této knize budeme hovořit primárně o dokumentech a jejich podepisování. O zprávách se zmíníme jen tam, kde bude třeba oba pojmy rozlišit.

1.2 Písemná, listinná a elektronická podoba dokumentu

Další termíny, o kterých bychom si měli říci, se již vztahují k formám dokumentů. Jde spíše o termíny z právní praxe, ale přesto se s nimi budeme často setkávat i v oblasti elektronického podpisu.

Například všude, kde bychom chtěli mluvit o „papírových" dokumentech, musíme správně hovořit o **listinné podobě dokumentu**, o **listinné formě dokumentu**, resp. **o listinném dokumentu**. Jejím protipólem je **elektronická podoba dokumentu** (resp. **elektronická forma dokumentu**, **elektronický**

dokument). V případě konverze dokumentů je proto na místě hovořit o **konverzi** z listinné do elektronické podoby, resp. o opačné konverzi (z elektronické do listinné podoby).[1] Tak o tom ostatně mluví i zákony a prováděcí předpisy (vyhlášky) kolem datových schránek.

Něco jiného je ale **písemná podoba**: ta znamená, že dokument je „napsaný", a tedy tvořený posloupností znaků (písmen, číslic a dalších znaků).[2] Požadavku na písemnou podobu, která se objevuje v mnoha zákonech a podzákonných předpisech, přitom lze vyhovět jak listinnou formou dokumentu, tak i jeho elektronickou formou.

Pamatujme si, že písemný dokument (písemnost) může mít jak listinnou, tak i elektronickou formu.

Někdy se ale můžeme setkat i s odlišnou terminologií. Například v oblasti archivnictví se mluví o **dokumentech v analogové podobě** (místo o listinných dokumentech), nebo o **dokumentech v digitální podobě** (místo o elektronických dokumentech).[3]

1.3 Podpis, elektronický podpis, digitální podpis

Písemný dokument (písemnost) je možné – a mnohdy i nutné – opatřit podpisem, neboli podepsat. Někdy k tomu stačí **vlastnoruční podpis**, ale někdy je nutný **ověřený vlastnoruční podpis** (ať již notářsky, soudně či úředně ověřený).

Obrázek 1-1
Vlastnoruční podpis Václava Klause

Jak vypadá vlastnoruční podpis, připojovaný k dokumentům v listinné podobě, si asi dovede představit každý. Pokud ale neznáte třeba vlastnoruční podpis prezidenta Václava Klause, můžete jej vidět na předchozím obrázku.

[1] S tím je ale poněkud ve sporu obvyklé pojetí termínu „listina", který je používán nezávisle na formě. Tj. hovoří se i o **listinách v elektronické formě.**

[2] Alternativou k písemné formě může být třeba forma **zvuku** (audia, tj. namluvený dokument) či **obrazu** (videa, tj. dokument natočený na kameru).

[3] Tyto pojmy používá zákon č. 499/2004 Sb. „o archivnictví a spisové službě".

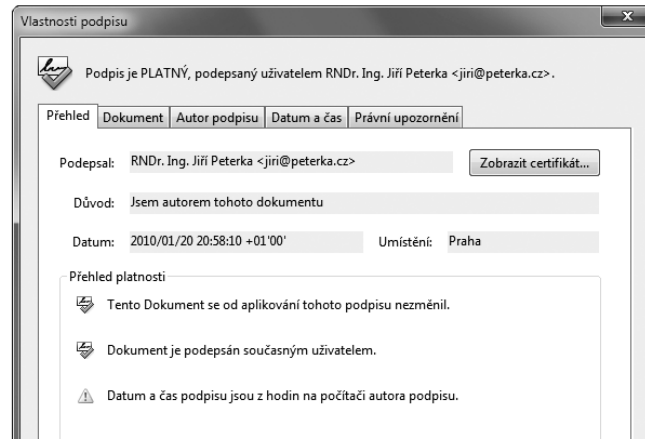
Pokud bychom (jakýkoli) vlastnoruční podpis dali ke zkoumání grafologovi, zabýval by se tím, jak je veden tah perem, jaký je sklon a tvar jednotlivých znaků, případně jaký inkoust byl při jeho tvorbě použit, na jakém papíře se podpis nachází atd.

V případě elektronického podpisu, který se připojuje k dokumentům v elektronické formě, by nic takového nemělo smysl zkoumat. Místo toho by se dalo hovořit o hodnotě elektronického podpisu a ověřovat, jestli je tato hodnota taková, jaká by měla být.

Elektronický podpis totiž ve své podstatě není ničím jiným, než (hodně velkým) číslem. Dokonce tak velkým, že by nebylo až tak šikovné ho psát jako binární číslo (jako posloupnost jedniček a nul). Takže pokud je někdy třeba ho zapsat tak, aby to bylo alespoň nějak srozumitelné pro člověka, využívá se k tomu nějaká efektivnější reprezentace (kódování), tak aby se vystačilo s méně znaky. Příkladem takového znázornění elektronického podpisu může být následující řetězec:

IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4BlrcnjaqbcKgNv+a5kr4537y8RC d+RHm75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAelws4S87UX80cLBtBcN6AACf11qymC2h+Rb2 j5SU+rmXWru+=QFMx

Pokud vám tento řetězec nic neříká, pak nezoufejte: v praxi nebudete s elektronickým podpisem pracovat v takovéto podobě (jako s číslem). Tak s ním pracují programy, které elektronický podpis na elektronickém dokumentu ověřují, a výsledek svého ověření dokáží svým uživatelům zobrazit v mnohem uživatelsky příjemnější (a také obsažnější) podobě. Příklad ukazuje následující obrázek, na kterém nám výsledek ověření elektronického podpisu sděluje program Adobe Reader:



Obrázek 1-2
Příklad vyhodnocení elektronického podpisu konkrétním programem (Adobe Reader)

V praxi se někdy můžeme setkat i s pojmem **digitální podpis**. Věcně by to bylo správnější označení[4] pro ten druh podpisu, kterým se v celé této knize budeme zabývat (a který má „povahu čísla“). Raději se ale přidržíme běžné praxe i dikce zákonů a vyhlášek, které pracují pouze s pojmem el**ektronický podpis**.[5]

1.4 Zaručený a uznávaný elektronický podpis

V dalších kapitolách se seznámíme s tím, že i elektronických podpisů existuje více druhů. Nás bude zajímat **zaručený elektronický podpis**, který už podle svého názvu dává „jisté záruky“. Nejvíce nás ale bude zajímat **uznávaný elektronický podpis**, jehož pojmenování zase můžeme vztáhnout k tomu, že pouze takovýto elektronický podpis nám „uzná“ úřad (orgán veřejné moci), pokud s ním budeme komunikovat elektronickou cestou.

Naopak nás nebude zajímat elektronický podpis „bez přívlastků“, protože ten je tak „slabý“, že negarantuje prakticky vůbec nic, a má spíše jen určitou informační hodnotu. Možná, že bychom ho ani neměli považovat za elektronický podpis (i když zákon tak činí).

Proto se již zde domluvme, že kdykoli budeme hovořit o elektronickém podpisu (bez dalšího upřesnění), budeme tím mít na mysli to, co zákon definuje jako zaručený elektronický podpis.

Stejně tak se domluvme, že když budeme hovořit o podpisu (bez dalšího upřesnění, a tedy i bez adjektiva „elektronický“), budeme mít také na mysli zaručený elektronický podpis.

1.5 Integrita, identifikace a nepopiratelnost

Budeme-li se podrobněji zabývat pouze zaručeným elektronickým podpisem, pak bychom měli vědět, jakého typu jsou záruky, které poskytuje. Je to vhodné už i proto, že vlastnoruční podpis takovéto záruky neposkytuje.

Jednou ze záruk, kterou zaručený elektronický podpis poskytuje, je tzv. **integrita dokumentu**. Tedy jeho neporušenost, ve smyslu celistvosti, neměnnosti.

---

[4] Přívlastek „digitální“ vypovídá o tom, že něco je zpracováváno číselně, resp. číslicově (digitálně), neboli je „vypočítáváno“, resp. zpracováváno formou výpočtu, a má proto charakter čísla. To platí právě pro ten druh podpisu, kterým se v celé této knize zabýváme. Naproti tomu přívlastek „elektronický“ vypovídá o tom, jak konkrétně reprezentujeme čísla, resp. číslice – a je alternativou například k přívlastku „optický“ (kdy číslice reprezentujeme opticky), „magnetický“, „mechanický“ apod.

[5] Někdy je jako digitální podpis označován takový podpis, který je založen na certifikátu a infrastruktuře veřejného klíče. A elektronický podpis jako něco obecnějšího, co může být založeno na certifikátu, ale také nemusí.

Abychom tomu ale rozuměli správně: ani (zaručený) elektronický podpis nedokáže zaručit, že podepsaný elektronický dokument nebude nějak pozměněn. Dokáže ale zaručit to, že pokud pozměněn bude, spolehlivě to poznáme (při vyhodnocování platnosti elektronického podpisu).

Jinými slovy nám (zaručený) elektronický podpis dává záruku, že se podepsaný dokument od okamžiku svého podpisu nezměnil. Nebo nám naopak řekne, že pozměněn byl – ale pak už se od něj nedozvíme, jak moc a kde byl pozměněn, zda jde o změnu v jednom jediném bitu, či zda není stejný ani jeden bit. Dozvíme se jen to, že k nějaké změně došlo, a že tedy nejde o přesně stejný dokument, jaký byl původně podepsán.

Zaručený elektronický podpis nám také pomáhá identifikovat „*toho, komu podpis patří*“. Tedy tzv. **podepsanou** či **podepisující osobu**, jak říkají zákony a vyhlášky. Poskytne nám určité údaje o identitě této osoby (například její jméno a příjmení), obecně se tomu říká **identifikace**.

Nepleťme si ale identifikaci s autentizací, jak se v praxi bohužel často děje. Identifikaci si můžeme představit jako odpověď na otázku „*kdo jsem?*“ či „*o koho jde?*“. V nejjednodušší podobě může být identifikace provedena zadáním uživatelského jména: tím nějakému systému sdělujeme, kým jsme. Oslovený systém by se ale měl přesvědčit, zda jsme skutečně tím, za koho se vydáváme, a ne nějakým podvodníkem, který se vydává za někoho jiného.

A tak nastupuje ještě **autentizace**, neboli ověření identity, resp. odpověď na otázku: „*jsem skutečně tím, za koho se vydávám?*“ V nejjednodušším případě může být autentizace provedena zadáním (správného) hesla. Sofistikovanější metody autentizace pak mohou využívat i techniky elektronického podpisu.

Zaručený elektronický podpis slouží i k poskytování důležité záruky, které se říká **nepopiratelnost** (někdy též: **neodmítnutelnost**): podepsaná osoba nemůže popřít, že podpis vytvořila ona (resp. nemůže odmítnout důsledky svého podpisu). To ovšem jen za podmínky, že tento zaručený elektronický podpis je dostatečně „kvalitní“,[6] v tom smyslu,že se můžeme spolehnout na to, co nám říká ohledně identity podepsané osoby.

U „pouhého“ zaručeného elektronického podpisu si ten, kdo podpis vytváří, ještě mohl nastavit údaje o identitě podepsané osoby tak, jak chtěl. Můžeme si to ukázat na příkladu zaručeného elektronického podpisu literární postavy Josefa Švejka, který vidíte na následujícím obrázku.[7]

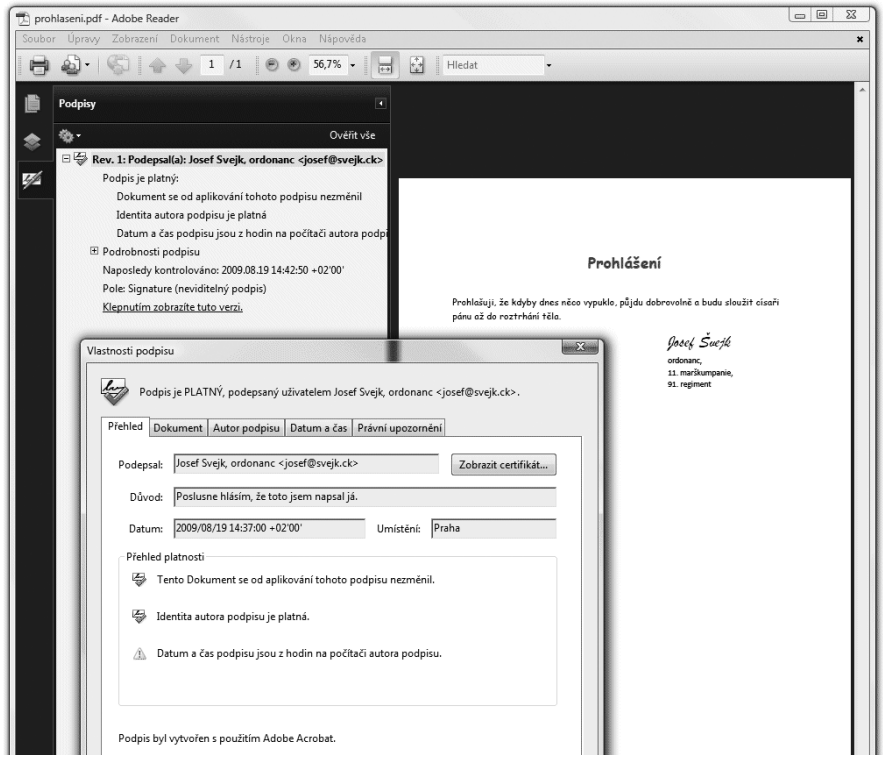
K tomu, abychom se mohli spolehnout na identitu podepsané osoby, nám tedy „pouhý“ zaručený elektronický podpis nestačí. K tomu již potřebujeme uznávaný elektronický podpis (zmiňovaný v předchozím odstavci), který je v tomto ohledu „silnější“. Na rozdíl od zaručeného elektronického podpisu klade přísné požadavky na zjištění a vyjádření identity toho, kdo je podepsanou osobou.

---

[6] Založený na kvalifikovaném certifikátu, viz dále.

[7] Soubor s popisovaným PDF dokumentem si můžete stáhnout na http://www.bajecnysvet.cz/priklady/selfsigned.php

Obrázek 1-3
Příklad zaručeného elektronického podpisu literární postavy Josefa Švejka



Uznávaný elektronický podpis literární postavy Josefa Švejka již nemůže existovat, protože nejde o skutečně existující fyzickou osobu.

1.6 Důvěrnost, autorizace, autenticita

Když už jsme u toho, jaké záruky poskytuje zaručený elektronický podpis, zastavme se také u těch, které naopak neposkytuje. Jde konkrétně o zajištění tzv. **důvěrnosti** (anglicky: **privacy**). Tím se rozumí zajištění toho, aby se s daným obsahem (v našem případě s obsahem dokumentu) nemohl seznámit nikdo nepovolaný.

Zdůrazněme si, že požadavek na zajištění důvěrnosti neznamená, že se předmětný obsah nesmí dostat do rukou někoho nepovolaného. To by byl podstatně silnější požadavek, který by se v běžné praxi – například v prostředí dnešního Internetu – dal realizovat jen velmi obtížně. Proto se u důvěrnosti netrvá na tom, aby se předmětný obsah nemohl dostat do nepovolaných rukou – ale trvá se na tom, aby

v takovém případě to oněm „nepovolaným rukám“ bylo k ničemu a nemohly se seznámit s tím, co má zůstat důvěrné.

V praxi se důvěrnosti dosahuje vhodným zašifrováním příslušného obsahu. To si budeme popisovat podrobněji v závěrečné kapitole (kapitole 8), ale již nyní si zdůrazněme, že jde o „něco jiného“ než je elektronický podpis: ten důvěrnost nezajišťuje.

> Zajištění důvěrnosti (skrze šifrování) ale může být kombinováno s elektronickým podepisováním: jakýkoli elektronický dokument či třeba e-mailovou zprávu, můžeme jak podepsat, tak i zašifrovat.

Jiným základním pojmem, se kterým se lze setkat (nejen) v souvislosti s elektronickým podpisem, je pojem **autorizace** (anglicky **authorization**). Velmi často se plete s pojmem autentizace, ale jde skutečně o něco úplně jiného: autentizace znamená prokazování vlastní identity, které jsme si již dříve přirovnali k odpovědi na otázku: „*jsem skutečně tím, za koho se vydávám?*“

U autorizace naopak jde o práva k určitým úkonům či aktivitám: někdo konkrétní chce provést určitý úkon (jako například: získat přístup k nějaké službě, provést změnu v konkrétním dokumentu, smazat nějaký soubor apod.), ale je otázkou, zda na to má či nemá právo. Autorizací v užším smyslu se pak rozumí udělení konkrétního práva k určitému úkonu (ve smyslu: „dotyčný je oprávněn provést změnu ….“). V širším smyslu se autorizací rozumí celá správa oprávnění, které mají konkrétní subjekty, včetně přidělování a odnímání těchto práv.

Ještě dalším zajímavým pojmem, se kterým se lze setkat v souvislosti s elektronickými dokumenty, je jejich **pravost**, resp. **autentičnost** či **autenticita**. Neformálně lze „pravost“ dokumentu chápat tak, že jde stále o „ten samý dokument“ a nikoli o nějaký jiný dokument, který by se za něj pouze vydával. Asi nejnázornější je protipříklad: pravost (autenticitu, autentičnost) porušíme tím, že na dokumentu něco změníme, nebo ho zaměníme nějakým úplně jiným dokumentem.[8]

Elektronický podpis nám s určením pravosti dokumentu může účinně pomoci, díky zajištění integrity dokumentu, opatřeného zaručeným elektronickým podpisem: neporušená integrita je důkazem, že dokument nebyl pozměněn či vyměněn.

Pravost (autenticita) dokumentu ale může být prokazována i jiným způsobem, který s elektronickým podpisem nemusí mít nic společného. Například notářskou úschovou, skrze svědecké výpovědi apod.

---

[8] Příkladem dokumentu, který není autentický, může být kolizní dokument (viz část 2.5.1)

1.7 Elektronické značky

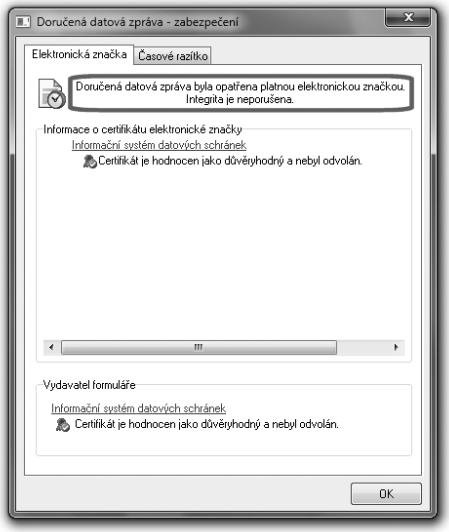
Elektronický podpis má ještě jeden zajímavý aspekt: je určen pouze lidem, resp. fyzickým osobám. Neexistuje žádný elektronický podpis právnické osoby, organizace, úřadu apod. Je to vlastně stejné jako u vlastnoručních podpisů: podepsat se (elektronicky) může jen fyzická osoba, která právě jedná jménem příslušné právnické osoby atd.

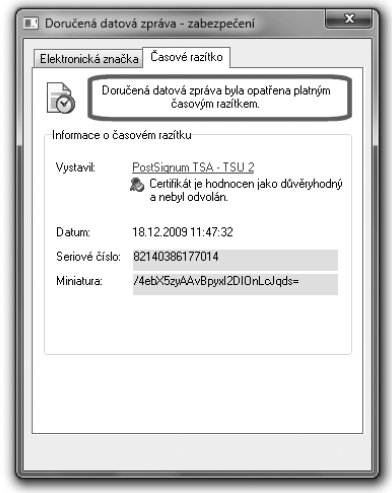
Praxe si nicméně vynutila obdobu elektronického podpisu, která již je dostupná i jiným subjektům, než jen fyzickým osobám. Konkrétně právnickým osobám (firmám, organizacím atd.), i organizačním složkám státu. Jde o tzv. **elektronickou značku**: ta je po technické stránce (zaručeným) elektronickým podpisem, a také je právně „podobná" zaručenému elektronickému podpisu. Navíc se u ní nepředpokládá, že by bezprostřední popud k jejímu vzniku musel vždy dávat člověk, který se nejprve seznámil s obsahem toho, co podepisuje (jako je tomu u elektronického podpisu).

Popud ke vzniku elektronické značky již může dávat i stroj, resp. program, bez přímé účasti člověka. Právní důsledky ale samozřejmě nenese takovýto stroj či program, nýbrž ten, kdo ho nastavil tak, aby značky vytvářel – a to je tzv. **označující osoba** (jako analogie podepisující či podepsané osoby).

Zdůrazněme si tedy, že zatímco zaručený elektronický podpis může vytvořit (a být tak podepsanou osobou) jen fyzická osoba, v případě elektronických značek už označující osobou nemusí být jen fyzická osoba, ale může to být i právnická osoba či organizační složka státu.

Obrázek 1-4
Příklad (uznávané) elektronické značky na datové zprávě v ISDS





Obrázek 1-5
Příklad (kvalifikovaného) časového razítka na datové zprávě v ISDS

Vedle elektronické značky (bez přívlastku), existuje i **uznávaná elektronická značka**, postavená na roveň uznávanému elektronickému podpisu.

1.8 Časová razítka

Dalším důležitým pojmem, se kterým se v praxi setkáme, je **časové razítko**. To je po technické stránce také (zaručeným) elektronickým podpisem, ale na rozdíl od něj je v něm uveden garantovaný údaj o čase jeho vzniku.[9] A tak časové razítko neslouží ani tak k podpisu, jako k „zachycení v čase", resp. k prokázání skutečnosti, že to, co je časovým razítkem opatřeno, již v okamžiku vzniku časového razítka existovalo.

Časové razítko tedy stvrzuje, že to, co je „orazítkováno", vzniklo „někdy před" časový okamžikem, uvedeným na časovém razítku. Už se ale neříká nic o tom, zda to bylo dříve o sekundy, minuty či třeba roky.

V praxi se ovšem používají spíše tzv. **kvalifikovaná časová razítka**, která jsou „silnější" než časová razítka (bez přívlastku), protože je vytváří kvalifikovaný poskytovatel (služby časových razítek). A na jeho služby a produkty (časová razítka i v nich obsažené časové údaje) se skutečně můžeme spolehnout.

Zrekapitulujme si nyní dosud uvedené základní pojmy a připomeňme si rozdíl mezi podpisem, značkou a razítkem:

Obrázek 1-6
Klasifikace podpisů, značek a razítek

elektronický podpis	*„bez přívlastku"*	podepsanou osobou může být pouze fyzická osoba
	zaručený	
	uznávaný	
elektronická značka	*„bez přívlastku"*	označující osobou může být jak fyzická osoba, tak i právnická osoba či organizační složka státu
	uznávaná	
časové razítko	*„bez přívlastku"*	
	kvalifikované	

[9] Jak si později řekneme, v rámci elektronického podpisu je také obsažen údaj o čase jeho vzniku. Ale tento údaj je převzat ze systémových hodin na počítači, kde podpis vzniká – a tyto hodiny si uživatel počítače mohl nastavit, jak chtěl, takže na časový údaj v rámci el. podpisu se nemůžeme spoléhat.

1.9 Klíče a asymetrická kryptografie

Dalším termínem, se kterým se u elektronických podpisů (ale i značek a časových razítek) běžně operuje, jsou **klíče**. Ve skutečnosti jsou to opět čísla, a tak má smysl hovořit o jejich délce (v bitech).

Důležité je ale jejich použití: jsou základní „ingrediencí" jak elektronických podpisů, tak i elektronických značek a časových razítek. Až si budeme popisovat vznik elektronického podpisu jakožto složitého výpočtu, uvidíme, že klíče (jako čísla) vstupují do tohoto výpočtu. A to jak při vzniku podpisu, tak i při jeho ověřování.

Celý princip elektronických podpisů ale staví na tom, že při vytváření podpisu (podepisování) a při ověřování (vyhodnocování platnosti) podpisu se používají různé klíče. Jde tedy o asymetrické řešení (kdy pracujeme s různými klíči), kvůli kterému musíme rozlišovat mezi veřejným a soukromým klíčem (kterému se někdy říká i privátní).[10]

Rozdíl mezi oběma druhy klíčů je přesně v tom, co říkají jejich přívlastky:

- **soukromý** (též: privátní) **klíč** si musíme pečlivě hlídat a rozhodně bychom ho neměli dávat někomu jinému.
- **veřejný klíč** naopak můžeme (a měli bychom) poskytnout komukoli, kdo si bude chtít ověřit platnost našeho podpisu.

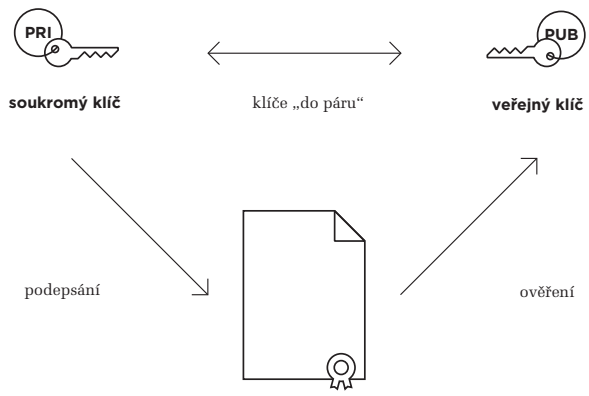
Důvodem je to, že právě soukromý klíč je tím, co potřebujeme pro vytváření vlastního elektronického podpisu. Je to „to", co nás jednoznačně identifikuje – a pokud bychom "to" (tedy náš soukromý klíč) dali někomu jinému, mohl by se podepisovat naším jménem. To jistě nechceme, a tak si musíme svůj soukromý klíč (či klíče) pečlivě střežit.

Naopak veřejný klíč je tím, co se používá pro vyhodnocování platnosti (ověřování) již existujícího elektronického podpisu – a na základě čeho se ten, kdo elektronický podpis vyhodnocuje, může také dopátrat, komu podpis vlastně patří. Takže chceme-li, aby se příjemce námi podepsaného dokumentu mohl ujistit o platnosti našeho podpisu (i o tom, že patří nám), musíme mu poskytnout svůj veřejný klíč.

A co tedy je **asymetrická kryptografie?** Je to hodně odborný termín, se kterým pracují specialisté – ale nám postačí vědět, že právě díky této „asymetrické kryptografii" je zajištěno, aby soukromý a veřejný klíč „byly do páru" (proto se také označují jako **párová data**) a fungovaly tak, jak jsme si právě naznačili. Asymetrická kryptografie zajišťuje dokonce i to, že když někomu dáme svůj veřejný klíč, že si z něj nedokáže vytvořit odpovídající soukromý klíč.

---

[10] V zákoně o elektronickém podpisu (zákoně č. 227/2000 Sb.) ale žádnou zmínku o klíčích nenajdeme. Zde se o nich mluví jako o **datech pro vytváření elektronického podpisu** v případě soukromého klíče, resp. jako **o datech pro ověřování elektronického podpisu** v případě veřejného klíče.



Obrázek 1-7
Představa využití soukromého a veřejného klíče

A proč že se mluví právě o asymetrické kryptografii a ne o kryptografii symetrické? I to souvisí s párovými daty, neboli s oběma klíči, které jsou u asymetrické kryptografie každý jiný (jeden soukromý a druhý veřejný). V případě **symetrické kryptografie** bychom museli pracovat se stejnými (symetrickými, resp. „nepárovými“) klíči, tedy vlastně se dvěma exempláři jednoho a téhož klíče – a to bychom žádný z nich nemohli dávat z ruky tak, jako to děláme u veřejného klíče. Proto se také takovémuto „symetrickému“ klíči říká **tajný klíč**.

1.10 Certifikáty

Vraťme se ale zpět k „asymetrickým“ klíčům: když někdo získá náš veřejný klíč, a s jeho pomocí si ověří platnost nějakého našeho elektronického podpisu, jak si může být jist, že jde skutečně o náš podpis? Přesněji: jak si může být jist, že onen veřejný klíč, použitý k ověření podpisu, je skutečně náš? Co když ve skutečnosti patří někomu úplně jinému, kdo by tímto způsobem chtěl vydávat svůj podpis za náš?

Jistě, pokud jsme dotyčnému předali náš veřejný klíč sami, hezky „z ruky do ruky“, pak není co řešit. Ale mnohem častější je situace, kdy jsme svůj veřejný klíč vyvěsili na nějakém veřejném místě v online světě (na nějaké veřejné nástěnce). Nebo – a to je zcela běžná praxe – jsme svůj veřejný klíč přiložili přímo k podepsanému dokumentu. Jak se potom může příjemce spolehnout na to, že skutečně jde o náš veřejný klíč?

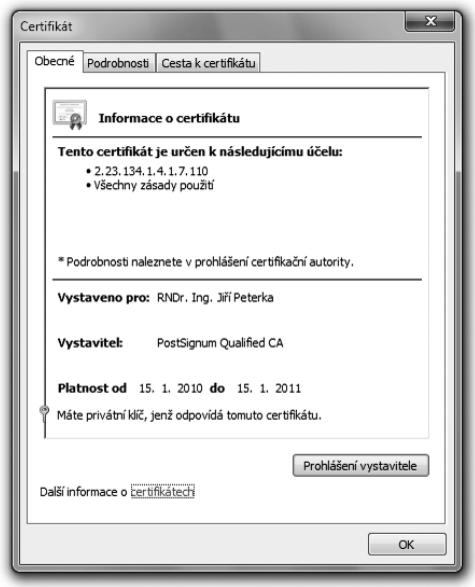
Řešení naštěstí není principiálně složité: stačí najít někoho třetího – nějakou dostatečně důvěryhodnou autoritu – která potvrdí, komu veřejný klíč patří. A aby to nemusela deklarovat pokaždé znovu, vystaví na to jakési opakovaně využitelné potvrzení, které také sama podepíše (opatří vlastním elektronickým podpisem, přesněji: značkou). Tomuto potvrzení se říká **certifikát**.

Certifikát je tedy potvrzením o tom, že konkrétní veřejný klíč (vložený do certifikátu jako jeho součást) patří té a té osobě (jejíž identita je popsána v certifikátu). Stvrzuje současně i to, že příslušná osoba je držitelem odpovídajícího soukromého klíče a má ho ve své (výlučné) moci.

Obrázek 1-8
Představa certifikátu

Certifikáty mohou být **osobními certifikáty**, tj. takovými, které mohou být vydávány jen fyzickým osobám.[11] Pro vytváření elektronických podpisů přitom připadají v úvahu pouze takovéto osobní certifikáty (ale ne všechny z nich).

Obrázek 1-9
Příklad (osobního) certifikátu jak jej zobrazují programy v prostředí MS Windows



Obvyklá formulace, že „*elektronický podpis byl vytvořen pomocí certifikátu*“, je proto striktně vzato nesmyslem (protože k vytvoření elektronického podpisu se používá soukromý klíč, který v certifikátu obsažen není).

[11] Naše certifikační autority je ale většinou neoznačují přívlastkem „osobní“. Místo toho hovoří o certifikátech „pro osobní použití“, nebo jen o certifikátech (bez přívlastku). Vydány ale mohou být jen fyzické osobě.

V praxi je ale tato formulace používána zcela běžně, jako určitá zkratka pro vyjádření toho, že „*k vytvoření podpisu byl použit ten soukromý klíč, který je do páru s veřejným klíčem, obsaženým v příslušném certifikátu*“.

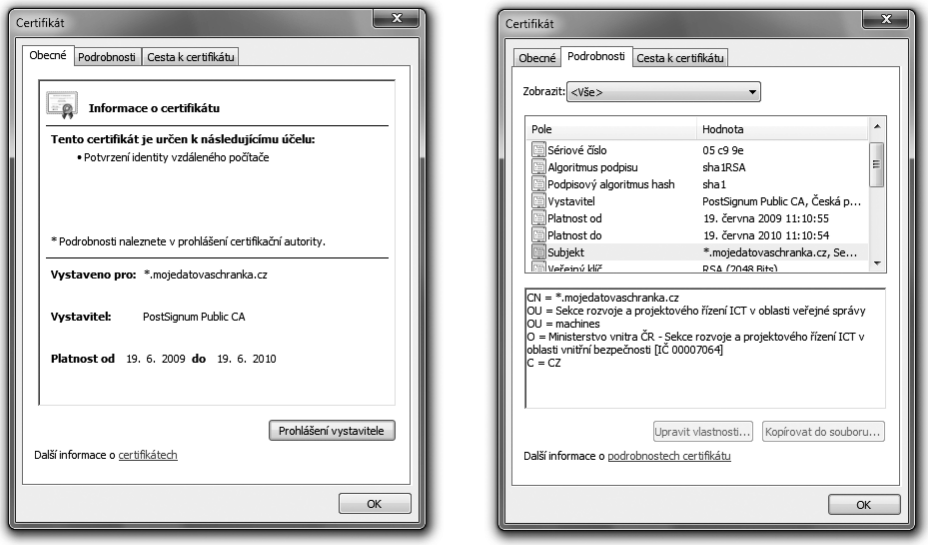
Zákony a nejrůznější vyhlášky ke stejnému sdělení používají ještě jinou formulaci, když hovoří o „*certifikátu, na kterém je elektronický podpis založen*“. Striktní dodržování tohoto slovního obratu ale leckdy komplikuje popis jinak jednoduchých a prostých skutečností nad hranici jejich srozumitelnosti.

V této knize si pro snazší a intuitivnější vyjadřování občas dopřejeme luxusu v podobě používání méně nepřesné formulace, že „*elektronický podpis byl vytvořen s využitím certifikátu*“. Nebo, když bude řeč o konkrétním certifikátu, že jde o „*certifikát, využitý k vytvoření elektronického podpisu*“. Obdobně pro elektronické značky a razítka.

Existují ale i takové certifikáty, které mohou být vydávány jak fyzickým osobám, tak i osobám právnickým (včetně orgánů veřejné moci) či organizačním složkám státu. Jde o tzv. **systémové certifikáty**, které mohou být využívány jak pro vytváření elektronických značek (ve smyslu předchozího terminologického zjednodušení), tak i pro vytváření časových razítek, ale stejně tak i pro další účely, jako je identifikace serverů, šifrování komunikace se servery (například v rámci SSL relací) apod.

Obrázek 1-10

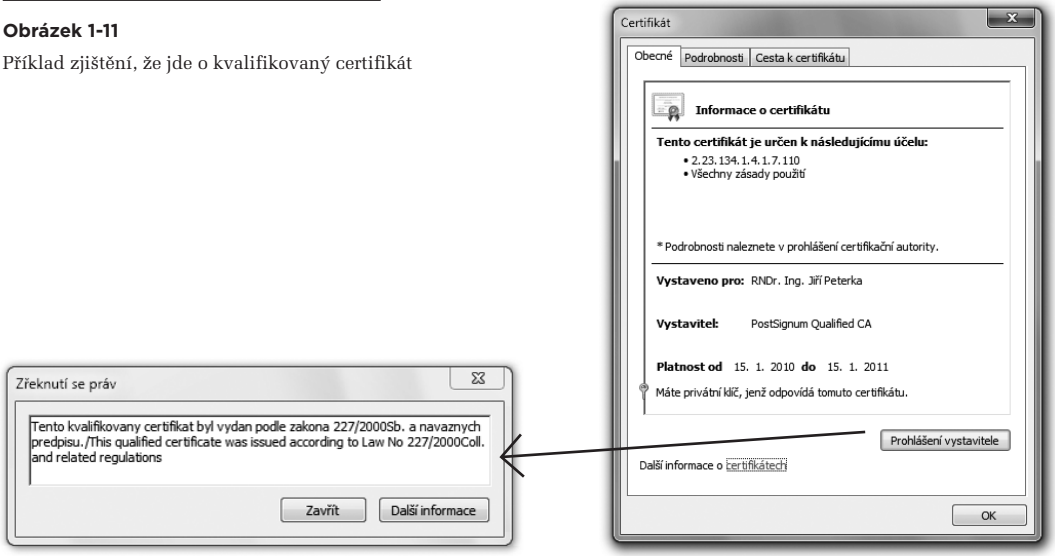
Příklad systémového certifikátu, který byl vystaven Ministerstvu vnitra, pro Informační systém datových schránek (ISDS), provozovaný na adrese mojedatovaschranka.cz



1.10.1 Komerční a kvalifikované certifikáty

Existují ale i jiná dělení certifikátů, podle jiných kritérií. Například na tzv. **komerční certifikáty** a **kvalifikované certifikáty**. Rozdíl mezi nimi je v tom, že požadavky na kvalifikované certifikáty a jejich obsah jsou vymezeny v zákoně, zatímco u komerčních certifikátů zákon jejich obsah nevymezuje.[12]

Obrázek 1-11
Příklad zjištění, že jde o kvalifikovaný certifikát



V praxi slouží kvalifikované certifikáty (ať již osobní či systémové) potřebám podepisování (resp. označování, při tvorbě elektronických značek či vytváření časových razítek) a ověřování podpisů, značek a razítek, zatímco pro všechny ostatní účely – jako je šifrování, přihlašování, prokazování identity a autentizace, zabezpečení apod., by měly být používány certifikáty komerční.

> Například pro (bezpečnější) přihlašování ke své datové schránce musí koncový uživatel použít svůj komerční osobní certifikát, zatímco spisová služba musí ke stejnému účelu použít komerční systémový certifikát. Pro případné podepsání dokumentu v elektronické podobě by fyzická osoba měla použít svůj kvalifikovaný osobní certifikát, zatímco „stroj“ musí pro vytvoření elektronické značky na dokumentu využít kvalifikovaný systémový certifikát.

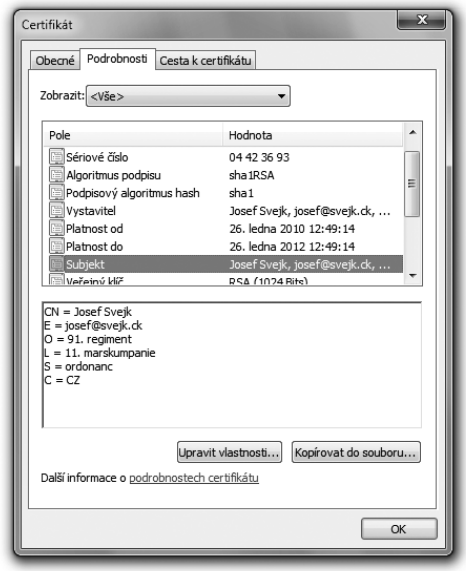
[12] Zákon ani nezná pojem „komerční certifikát“, v praxi se pod tento pojem zahrnují všechny certifikáty, které nejsou kvalifikované. Ale také ne vždy: někdy jsou například emailové certifikáty (či testovací certifikáty) chápány jako samostatné druhy certifikátů. Zde ale budeme vycházet z předpokladu, že „komerční“ jsou všechny certifikáty, které nejsou kvalifikované.

Mezi komerční patří i některé poměrně speciální druhy certifikátů, jako například **testovací certifikáty**, určené na „hraní“ (resp. testování), případně **emailové certifikáty**, dokládající právě a pouze možnost přístupu k určité emailové adrese, případně ještě další druhy certifikátů.

Příkladem certifikátu, který není kvalifikovaný – a který (v rámci komerčních certifikátů) musíme hodnotit jen jako testovací, neboli „na hraní“ – může být certifikát na dalším obrázku, vydaný již zmiňované literární postavě Josefa Švejka. Příklad jeho využití jsme si již ukazovali (pro elektronický podpis, který byl zaručený, ale nikoli uznávaný).

Zdůrazněme si ale to podstatné: že i certifikáty se liší v tom, jak dalece můžeme důvěřovat jejich obsahu. U testovacích certifikátů, jakým je právě certifikát (literární postavy) Josefa Švejka na obrázku, jejich obsahu věřit nemůžeme.

Obrázek 1-12
Příklad (testovacího) certifikátu, znějícího na literární postavu Josefa Švejka



Na opačném konci pomyslné škály stojí certifikáty kvalifikované, jejichž obsahu můžeme věřit nejvíce. Možnost důvěřovat obsahu určitého certifikátu je dána především tím, jak moc jeho vydavatel zkoumal identitu toho, komu certifikát vydává, a jak moc je ochoten za zjištění této identity odpovídat. U kvalifikovaných certifikátů tuto identitu zkoumá nejdůkladněji, a také za její správné zjištění ručí v nejvyšší možné míře. U certifikátů testovacích naopak nejméně. Vlastně vůbec.

Obrázek 1-13
Představa klasifikace certifikátů

certifikáty	**osobní**	**kvalifikované (pro podepisování)**
		komerční (včetně testovacích, emailových, ...)
	systémové	**kvalifikované (pro označování)**
		komerční (včetně testovacích, pro šiftrování, ...)

1.11 Certifikační autority

Ten, kdo certifikáty vydává, je běžně označován jako tzv. **certifikační autorita**, zkratkou **CA**. V terminologii zákonů a vyhlášek je to ale **poskytovatel certifikačních služeb**.

Jak později uvidíme, i certifikačních autorit (poskytovatelů certifikačních služeb) existuje celá široká škála. Certifikační autoritu si například můžete provozovat sami na svém počítači a vydávat si své vlastní certifikáty (tzv. „s vlastním podpisem"). Stejně tak může certifikační autoritu provozovat třeba váš provider či váš zaměstnavatel, a jako zákazníkovi či zaměstnanci vám vydat certifikát, skrze který se mu budete prokazovat (že jste to skutečně vy).

Ještě známějším příkladem mohou být certifikační autority provozované bankami, s tím že jimi vydávané certifikáty jsou využívány pro zabezpečení jejich internetbankingu.

1.11.1 Kvalifikované a akreditované certifikační autority

Nás ale budou nejvíce zajímat tzv. **kvalifikované certifikační autority**. To jsou ty, které vydávají kvalifikované certifikáty (přesně definované zákonem), a které splňují všechny další požadavky zákona na své vlastní fungování.[13]

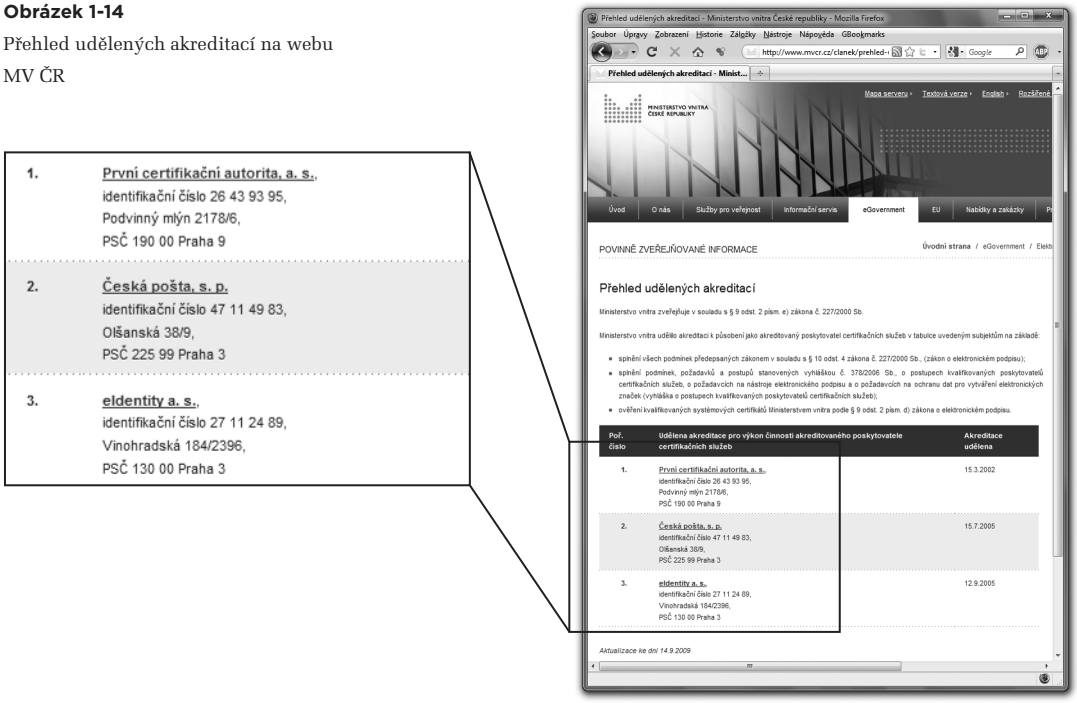
> Kvalifikované certifikáty mohou vydávat pouze takovéto kvalifikované certifikační autority. Komerční certifikáty již mohou vydávat všechny certifikační autority.

Kterákoli z kvalifikovaných certifikačních autorit přitom může požádat stát, aby prověřil, zda skutečně splňuje všechny požadavky zákona – a pokud ano, udělil této certifikační autoritě své „posvěcení" formou tzv. **akreditace**.

Akreditací se z kvalifikovaných certifikačních autorit stávají tzv. **akreditované certifikační autority**, alias **akreditovaní poskytovatelé certifikačních služeb**.

[13] Včetně toho, že státu oznámily, že vydávají kvalifikované certifikáty.

Obrázek 1-14
Přehled udělených akreditací na webu MV ČR



To samozřejmě neznamená, že by všechny ostatní kvalifikované certifikační autority byly automaticky nějak nedůvěryhodné. Akreditaci je vhodné chápat spíše jako nutný (zákonem stanovený) předpoklad, související s požadavkem:

> Chcete-li komunikovat se státem, resp. s orgány veřejné moci, musíte používat tzv. uznávané elektronické podpisy.

Pro uznávané elektronické podpisy je totiž třeba používat právě kvalifikované certifikáty, vydané akreditovanou certifikační autoritou. To je ostatně i hlavní (a vlastně jediný) rozdíl mezi zaručeným a uznávaným elektronickým podpisem.

Jinak jsou požadavky, kladené zákonem na kvalifikované a akreditované certifikační autority, úplně stejné. Splňovat musí to samé. Jen ty druhé na to „mají papír“ díky tomu, že samy a dobrovolně požádaly stát, aby zkontroloval (a průběžně kontroloval), že požadavky skutečně splňují.

> V České republice nebyla v roce 2010 žádná kvalifikovaná certifikační autorita, která by nebyla současně akreditovaná. Jinými slovy: všechny (tři) kvalifikované certifikační autority byly současně i akreditované.

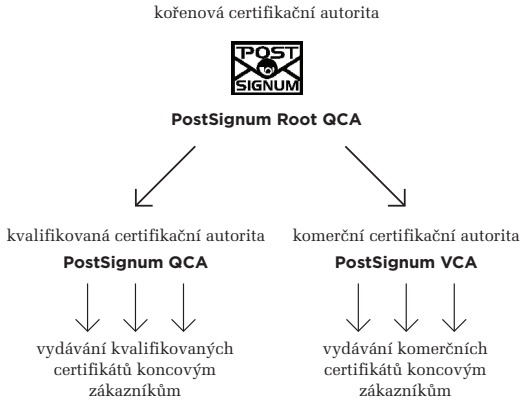
1.11.2 Kořenové a podřízené certifikační autority

Certifikační autority, a to zejména ty akreditované, přitom nemusí být (a nebývají) „homogenní“, ve smyslu svého organizačního členění. Z praktických důvodů jsou naopak často vnitřně členěny, na **kořenové autority**, které jakoby vše zastřešují, a **podřízené autority** (někdy též **zprostředkující autority**), které teprve vydávají různé druhy certifikátů koncovým zákazníkům.[14]

Takovéto hierarchické členění používá například certifikační autorita **PostSignum**, která měla do konce roku 2009 jednu kořenovou certifikační autoritu („Certifikační autoritu PostSignum“, PostSignum Root QCA) a dvě podřízené autority:

- kvalifikovanou certifikační autoritu (PostSignum QCA, též PostSignum Qualified CA), která vydává kvalifikované certifikáty
- komerční certifikační autoritu (PostSignum VCA, též PostSignum Public CA), která vydává komerční certifikáty

Obrázek 1-15
Vnitřní členění CA PostSignum do roku 2009

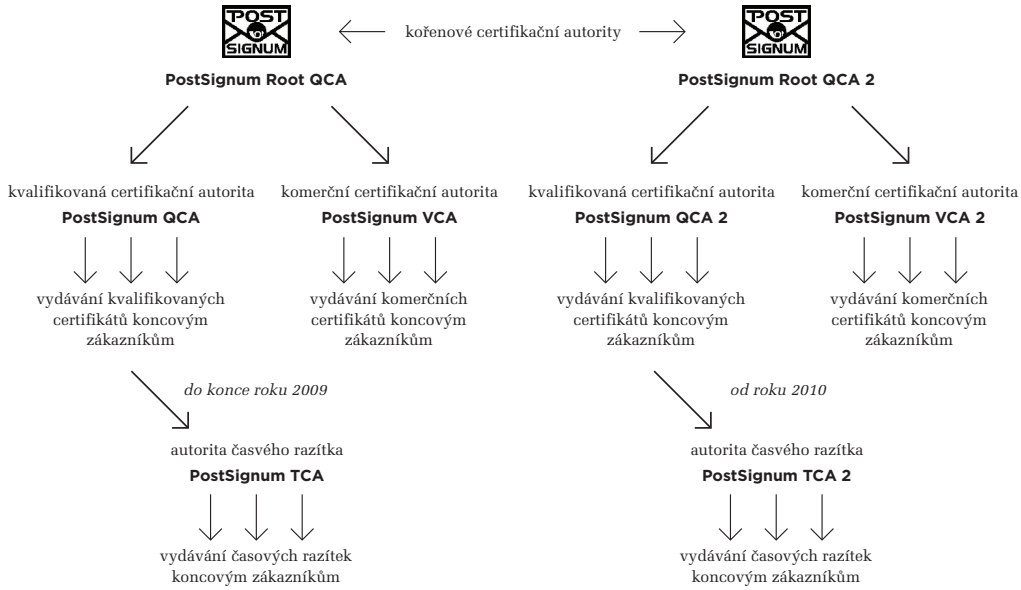


Počátkem roku 2010 pak, v souvislosti s přechodem na novou hašovací funkci SHA-2, svou vnitřní strukturu jakoby zdvojila: přidala novou kořenovou autoritu (PostSignum Root QCA 2), novou kvalifikovanou certifikační autoritu (PostSignum QCA 2, též PostSignum Qualified CA 2) a novou komerční certifikační autoritu (PostSignum VCA 2, též PostSignum Public CA 2). Viz následující obrázek, který již ukazuje i další podřízené autority, konkrétně pro vydávání časových razítek (PostSignum TSA).

[14] Při tomto členění vydávají kořenové certifikační autority certifikáty pouze svým podřízeným (zprostředkujícím) certifikačním autoritám.

Obrázek 1-16

Vnitřní členění CA PostSignum od roku 2010

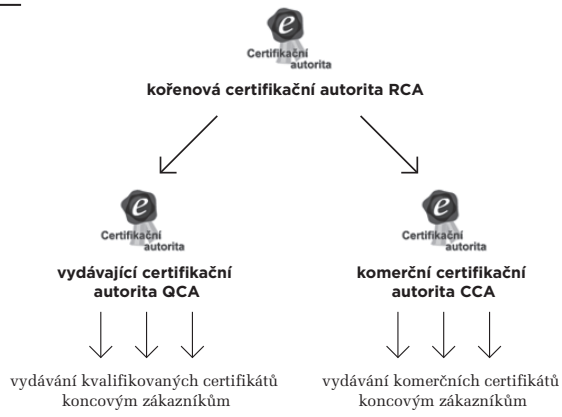


Hlavní rozdíl mezi původními a „dvojkovými“ autoritami PostSignum je přitom v tom, zda používají starší hašovací funkci SHA-1 (původní autority) nebo novou SHA-2 (nové „dvojkové“ autority).

Obdobně hierarchicky členěnou strukturu má i další akreditovaná certifikační autorita, **eIdentity**, viz obrázek.

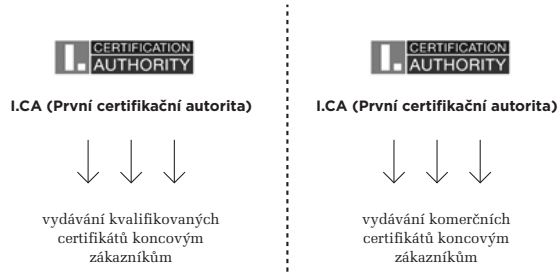
Obrázek 1-17

Vnitřní členění CA eIdentity



Naproti tomu certifikační autorita **I. CA (První certifikační autorita)** používá „ploché“ uspořádání:

Obrázek 1-18
Vnitřní členění I.CA



1.12 PKI, aneb infrastruktura veřejného klíče

Snad nejvýznamnějším atributem každého certifikátu je jeho důvěryhodnost. Tedy otázka toho, jak dalece můžeme věřit tomu, co je v certifikátu obsaženo a uvedeno.

Připomeňme si, že v certifikátu je obsažen veřejný klíč a je zde uvedena i identita osoby, které tento veřejný klíč patří. Tato osoba také má ve svém držení odpovídající soukromý klíč.

Na otázku důvěryhodnosti konkrétních certifikátů přitom budeme narážet zcela rutinně: kdykoli budeme ověřovat platnost nějakého elektronického podpisu (či značky nebo razítka), budeme k tomu potřebovat údaje, obsažené v certifikátu.

Certifikát nejčastěji získáme spolu s tím, co je podepsáno (spolu s podepsaným dokumentem). A pokud snad ne, musíme si ho odněkud stáhnout sami. Nicméně v obou případech budeme potřebovat vědět, zda je certifikát důvěryhodný a zda se můžeme na jeho obsah spoléhat.

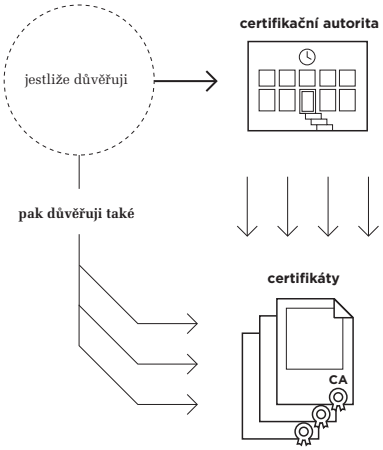
Důvěryhodnost každého certifikátu samozřejmě můžeme posuzovat individuálně, pro každý jednotlivý certifikát, a to na základě takových informací, jaké máme k dispozici. Třeba pokud nám někdo, koho dobře známe a v koho máme důvěru, sám předá konkrétní certifikát a prohlásí ho za svůj vlastní, asi můžeme tento certifikát zařadit mezi ty, kterým budeme důvěřovat. Pak nám může být celkem jedno, kdo certifikát vydal. Mohl to být třeba sám dotyčný, skrze nějakou vlastní – „na koleně“ provozovanou – certifikační autoritu.

V praxi bychom ale touto cestou daleko nedošli. Těžko bychom se totiž dokázali osobně (a dopředu) setkat se všemi osobami, se kterými budeme chtít nějak elektronicky komunikovat, či od nich jen přijímat elektronicky podepsané dokumenty. Navíc by nám to nejspíš nebylo k ničemu, protože bychom tyto osoby tak jako tak nejspíše neznali, a tak bychom ani nemohli důvěřovat těm certifikátům, které by nám předali.

Potřebovali bychom nějakého důvěryhodného prostředníka, který by nám certifikáty různých osob předával a sám se zaručil za autenticitu (pravost) těchto certifikátů. A tím i za identitu osob, kterým byly certifikáty vydány. Z předchozího už jistě tušíte, že takovýmto prostředníkem by měla být sama certifikační autorita, která certifikát vydala.

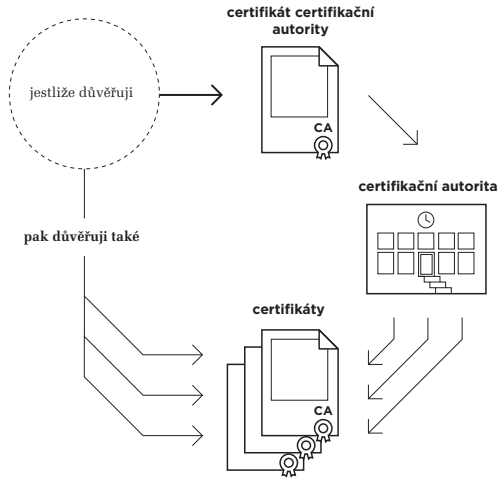
U certifikátů a certifikačních autorit navíc platí něco, co bychom mohli označit jako „delegaci důvěry“: když budu důvěřovat nějaké konkrétní certifikační autoritě, mohu důvěřovat i všem certifikátům, které tato certifikační autorita vydala. Což je jinými slovy totéž, jako tvrzení že důvěryhodnost konkrétního certifikátu odvozuji od důvěryhodnosti jeho vydavatele. Nicméně první z obou pohledů je vhodnější pro pochopení jednoho velmi praktického aspektu: stačí námjeden úkon – a to vyjádření důvěry certifikační autoritě – abychom tím vyjádřili důvěru všem certifikátům, které tato certifikační autorita vydala (a již jim nemuseli vyjadřovat důvěru individuálně).

Obrázek 1-19
Představa vyjádření důvěry všem certifikátům, které vydala konkrétní certifikační autorita



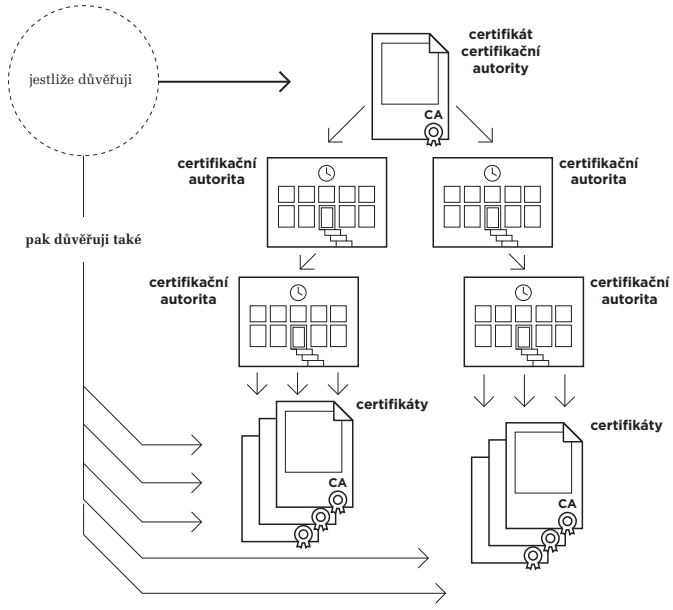
V praxi by ale nebylo příliš praktické vyjadřovat svou důvěru konkrétní certifikační autoritě „jako takové“. Nebylo by ani moc jasné, jak to vlastně udělat (po technické stránce). Naštěstí i zde existuje řešení, založené na tom, že i sama certifikační autorita používá k vydávání certifikátů nějaký vlastní certifikát. Musí, protože každý vydaný certifikát podepisuje svým vlastním elektronickým podpisem (přesněji opatřuje svou elektronickou značkou). K vyjádření důvěry certifikační autoritě pak stačí vyjádřit důvěru tomu jejímu certifikátu, který k tomu používá. Představu ukazuje následující obrázek.

Obrázek 1-20
Představa vyjádření důvěry certifikátu certifikační autority



Na celém systému vyjadřování důvěry je zajímavé a důležité také to, že ji lze „dále řetězit“: když někomu vyjádřím důvěru, a ten někdo pak sám vyjádří důvěru někomu dalšímu, mohu i já důvěřovat „tomu dalšímu“. V terminologii certifikačních autorit to znamená, že když považuji za důvěryhodnou jednu certifikační autoritu, a ta prohlásí za důvěryhodnou jednu či více dalších autorit (tj.: zaručí se za jejich důvěryhodnost), pak i já mohu považovat za důvěryhodné tyto další autority.

Obrázek 1-21
Představa stromu důvěry

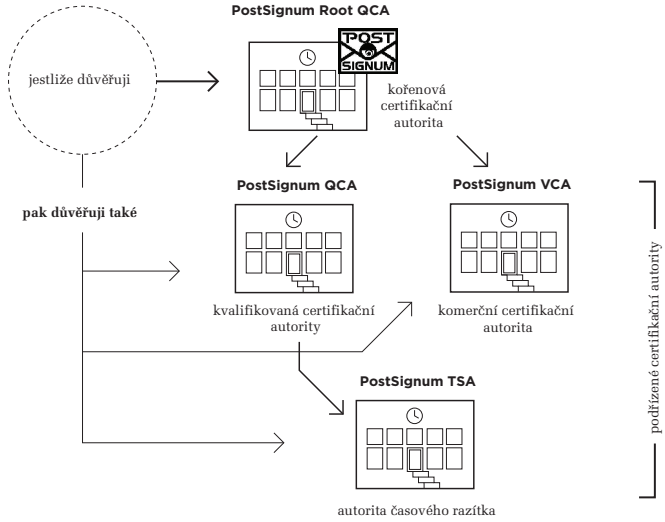


Vše se tedy dá zobecnit, do celého **stromu důvěry**: v jeho kořeni je jeden certifikát (tzv. **kořenový certifikát**), který odpovídá jedné (typicky: kořenové) certifikační autoritě. Od něj se odvíjí důvěra v další certifikáty (všechny vnitřní uzly stromu, tj. „podřízené“ certifikační autority, resp. jejich certifikáty) i všechny koncové uzly (certifikáty koncových uživatelů). Pokud pak někdo vyjádří svou důvěru příslušnému kořenovému certifikátu, fakticky tím vyjadřuje svou důvěru rovnou celému stromu.

Vše přitom sleduje jeden hlavní cíl, kterým je zjednodušit vyjadřování důvěry: uživatelé dostávají jeden „pevný bod“, v podobě kořenového certifikátu – a skrze něj mohou „fixovat“ svou důvěru v celý strom certifikátů (vyjádřením důvěry kořeni stromu, viz výše).

Představme si to na již zmiňovaném příkladu certifikačních autorit PostSignum: pokud budeme důvěřovat jejich kořenové certifikační autoritě (PostSignum Root QCA), budeme důvěřovat i všem jejím podřízeným certifikačním autoritám: kvalifikované (PostSignum QCA), komerční (PostSignum VCA), i autoritě časového razítka (PostSignum TSA).

Obrázek 1-22
Představa vyjadřování důvěry v CA PostSignum



> Jelikož ale PostSignum má od roku 2010 dvě různé kořenové certifikační autority (PostSignum Root QCA a PostSignum Root QCA 2), a ty nejsou zastřešeny žádnou společnou „nadřazenou“ autoritou, je nutné vyjadřovat jim důvěru samostatně, každé zvlášť.

V praxi, kdy máme více různých certifikačních autorit, jde typicky o více stromů důvěry a tomu odpovídající počet kořenových certifikátů. Dohromady se pak hovoří o celé **infrastruktuře veřejného klíče** (anglicky **PKI, Public Key Infrastructure**), neboť jejím účelem je zajistit dostatečně důvěryhodný systém distribuce veřejných klíčů (obsažených v certifikátech).

1.12.1 Důvěra, nedůvěra a nedostatek informací o důvěryhodnosti

Vyjadřování důvěry certifikátům je nesmírně důležitým (ba přímo kardinálním) aspektem elektronického podpisu. To proto, že právě od důvěryhodnosti konkrétních certifikátů se odvozuje důvěra a platnost konkrétních elektronických podpisů, značek či razítek. Je to ostatně logické: máme-li se spoléhat na nějaký podpis (či značku nebo razítko), potřebujeme spolehlivě vědět, čí podpis (či značka, razítko) to je. A to nám spolehlivě řekne pouze dostatečně důvěryhodný certifikát.

V praxi je vždy na uživateli, aby správně vyjádřil svou důvěru konkrétním certifikátům či celým stromům certifikátů, ve výše uvedeném smyslu. A pokud se zmýlí, je to „na něm" a on ponese následky za svou chybu.

V souvislosti s certifikáty si ale musíme uvědomit, že při vyjadřování důvěry neplatí jednoduchá dichotomie: že certifikát je buďto důvěryhodný, nebo naopak nedůvěryhodný. Místo toho musíme pracovat se třemi možnostmi:

- **certifikát je důvěryhodný**
- **certifikát je nedůvěryhodný**
- **nemáme dostatek informací k hodnocení důvěryhodnosti certifikátu.**

Pro první dvě možnosti musíme vždy mít nějaký konkrétní důvod. Aby mohl být nějaký certifikát považován za důvěryhodný, musí být buďto prohlášen za důvěryhodný přímo tento certifikát, nebo musí „patřit" do některého stromu důvěry, jehož kořen (kořenový certifikát) byl prohlášen za důvěryhodný.

Podobně pro nedůvěryhodnost: i zde buďto musí být prohlášen za nedůvěryhodný přímo daný certifikát, nebo musí „patřit" do některého stromu (ne)důvěry, jehož kořen byl prohlášen za nedůvěryhodný. Pokud nenastane ani jedna z těchto dvou možností, zbývá ještě ona třetí možnost: že nemáme dostatek informací k tomu, abychom dokázali zhodnotit důvěryhodnost daného certifikátu. V praxi bývá tato třetí možnost poměrně častá.

1.12.2 Vyjadřování důvěry v certifikát

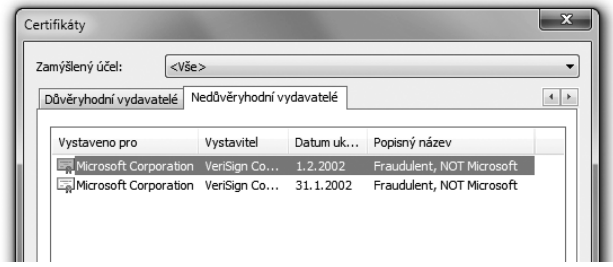
Konkrétní způsob, jakým „na svém počítači" vyjádříme důvěru konkrétnímu certifikátu, ať již kořenovému či jinému, je dán tím, jakým způsobem pracují s certifikáty nejrůznější programy: uchovávají si je ve speciálních **úložištích certifikátů** (anglicky **certificate store**).

V prvním přiblížení bychom mohli říct, že jde o úložiště důvěryhodných certifikátů, a že obecně platí, že když je nějaký certifikát uložen v takovémto úložišti, je považován za důvěryhodný.

Praxe je ovšem taková, že úložiště mohou být vnitřně strukturována do různých složek a různé složky mohou mít také různý význam. Většina z nich „vyjadřuje důvěru" těm certifikátům, které jsou do příslušné složky přidány (uloženy, nainstalovány). Ale mohou existovat i složky s opačným významem: když do nich umístíme konkrétní certifikát, vyjadřujeme mu tím nedůvěru.

> To je ostatně i příklad systémového úložiště certifikátů, které vytváří operační systém MS Windows a které má složku pro nedůvěryhodné certifikáty, viz obrázek.

Obrázek 1-23
Příklad dvou nedůvěryhodných certifikátů (umístěných v systémovém úložišti MS Windows, v části pro nedůvěryhodné certifikáty).



Správně tedy musíme rozlišovat, jak konkrétně je nějaké úložiště strukturováno a naplněno: je-li konkrétní certifikát umístěn v takové složce úložiště, která představuje vyjádření důvěry, pak je tento certifikát považován za důvěryhodný. Jde-li o kořenový certifikát, umístěný ve složce pro kořenové certifikáty, je za důvěryhodný považován celý příslušný strom certifikátů. A naopak: pokud je nějaký certifikát umístěn v takové složce, která představuje vyjádření nedůvěry, je za nedůvěryhodný považován jak tento certifikát, tak i celý jeho „podstrom".

Pokud ale není konkrétní certifikát umístěn v žádné ze složek právě používaného úložiště certifikátů, nevyplývá z toho nic o jeho důvěryhodnosti! Takže program, který s daným úložištěm certifikátů pracuje, nemá podle čeho posoudit jeho důvěryhodnost. Jde tedy o třetí možnost v již dříve diskutovaném smyslu (že certifikát je buďto důvěryhodný, nebo nedůvěryhodný, nebo „nevíme").

Na adresu úložišť certifikátů si ještě řekněme, že každý uživatelský program (aplikace) může používat své vlastní úložiště certifikátů. Může, ale nemusí – některé programy totiž dokáží svá úložiště sdílet.

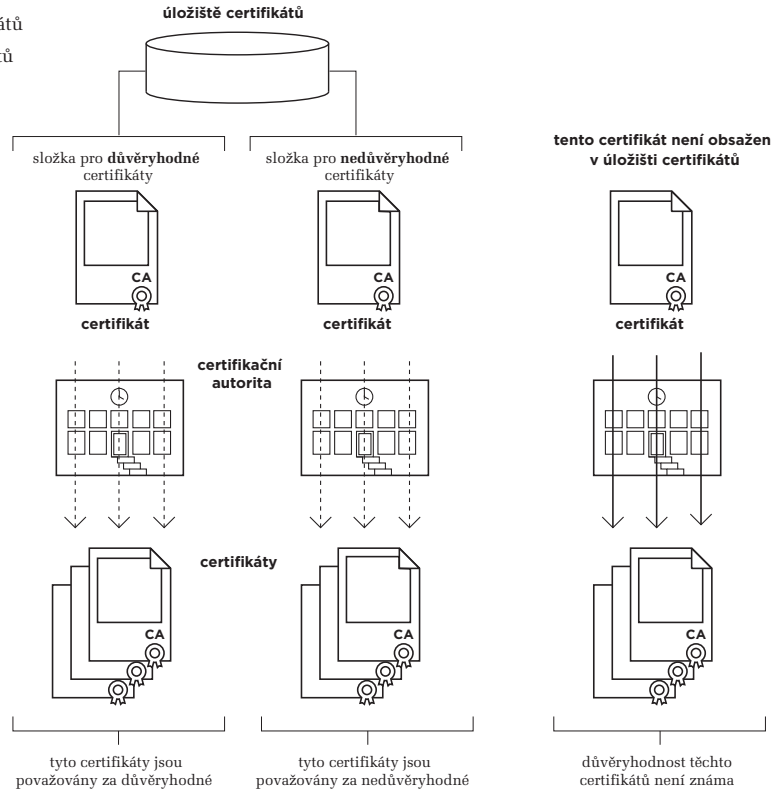
> Například programy z produkce Microsoftu používají systémové úložiště certifikátů, které vytváří operační systém MS Windows. Jiné programy, jako třeba Adobe Reader, Adobe Acrobat či prohlížeč Firefox, mají vlastní úložiště. Ale třeba právě Adobe Reader či Acrobat dokáží používat i systémové úložiště, podle toho jak jsou nastaveny.

Obecně tak musíme počítat s tím, že úložišť certifikátů je více a jako uživatelé se musíme starat o správné „naplnění" všech těch úložišť, se kterými pracují námi používané programy.

Vědět o existenci všech relevantních úložišť (a o tom, který program používá které úložiště), je pro běžnou praxi o to důležitější, že každé úložiště je nějak „předvyplněno" takovými certifikáty, které autoři příslušných programů považují za důvěryhodné. Tím je fakticky předjímáno, co a jak má být považováno za důvěryhodné i uživateli. Což ale nemusí vždy a přesně odpovídat představám uživatelů.

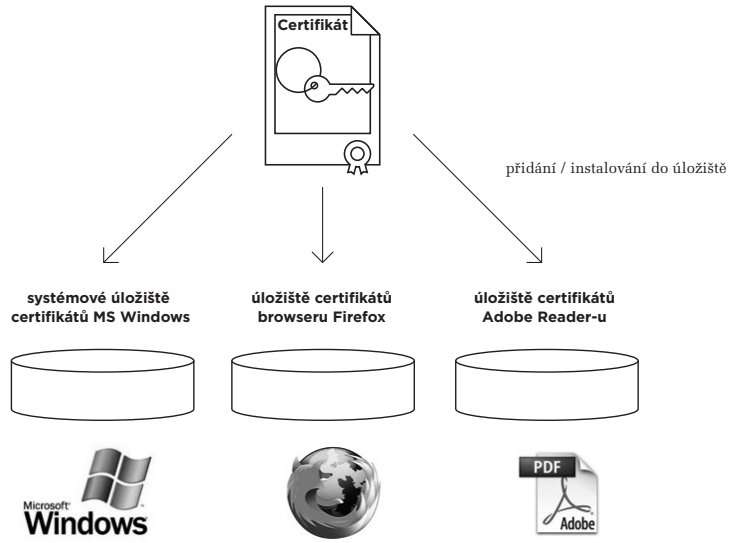
Nejčastěji v tom smyslu, že uživatel má důvod považovat za důvěryhodné i další certifikáty (resp. celé stromy certifikátů), ale ty „od výrobce“ v příslušném úložišti obsaženy nejsou. Pak je na něm, aby si je do úložiště přidal.

Obrázek 1-24
Představa důvěryhodnosti certifikátů podle umístění v úložišti certifikátů



Typickým a častým problémem je pak to, že v „počáteční výbavě“ úložišť certifikátů nebývají všechny kořenové certifikáty všech tuzemských akreditovaných certifikačních autorit. To ale způsobuje, že k hodnocení některých certifikátů, vydaných těmito akreditovanými certifikačními autoritami, nemají příslušné programy dostatek informací.

Obrázek 1-25
Představa více úložišť a potřeba jejich samostatného naplnění



1.12.3 Hierarchie certifikátů a certifikační cesty

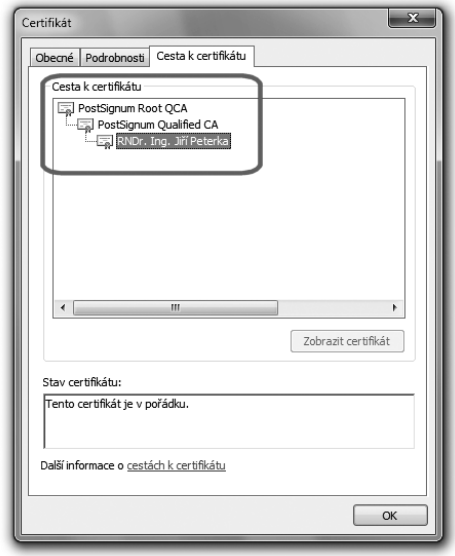
Aby výše popsaný princip vyjadřování důvěry mohl v praxi fungovat a důvěra v konkrétní certifikáty mohla být odvozována od jejich příslušnosti do konkrétního stromu důvěry, musí každý certifikát obsahovat určité minimální údaje, sloužící těmto účelům.

Konkrétně musí obsahovat údaj o svém vydavateli, resp. vystaviteli. Tedy o certifikační autoritě, která certifikát vydala (vystavila). Tento údaj je současně i odkazem na **nadřazený certifikát**, ve smyslu stromovitého uspořádání stromu důvěry, který vydavatel použil při vystavování daného certifikátu (pro jeho podepsání).

Skrze tento údaj (o nadřazeném certifikátu) je pak možné dohledat celou tzv. **certifikační cestu** k některému z kořenových certifikátů, a podle něj určit důvěryhodnost posuzovaného certifikátu. Příklad vidíte na obrázku na další stránce: jde o konkrétní certifikát a jeho certifikační cestu. Ta ukazuje, že certifikát byl vydán certifikační autoritou PostSignum, konkrétně její podřízenou kvalifikovanou autoritou QCA (PostSignum Qualified CA).

Certifikát této podřízené autority (PostSignum Qualified CA) zase byl vydán kořenovou certifikační autoritou PostSignum (tj. PostSignum Root QCA), a podepsán s využitím (kořenového) certifikátu této (kořenové) certifikační autority. Důležité také je, že dohledání certifikační cesty za nás může provést program, který používáme k ověřování platnosti elektronických podpisů. Jen ho musíme správně informovat o důvěryhodnosti příslušných certifikátů, pomocí jejich uložení do (správné části) toho úložiště certifikátů, které daný program používá.

Obrázek 1-26
Příklad certifikační cesty konkrétního certifikátu



1.13 Alternativní koncepce elektronického podpisu

Abychom dostatečně docenili celý koncept elektronických podpisů, používaných v praxi a popisovaných v této knize, naznačme si alespoň letmo, jaké k němu existují alternativy. Tedy co a jak by mohlo být jinak. Tím, co by se dalo „udělat jinak“, je už samotné vydávání certifikátů, a především tedy stvrzení vazby mezi veřejným klíčem a identitou toho, komu tento veřejný klíč patří.

Až dosud jsme předpokládali poměrně rigidní a „centralizované“ řešení, založené na existenci certifikačních autorit a celé infrastruktury veřejného klíče (PKI). Spolu s tím jsme předpokládali, že certifikáty vydávají certifikační autority, coby důvěryhodné třetí strany, které také ručí za obsah vystaveného certifikátu.

Naši důvěru v konkrétní certifikát a jeho obsah jsme pak odvozovali od důvěry v tuto certifikační autoritu, případně v její nadřazenou certifikační autoritu – protože, jak již víme, certifikační autority mohou v rámci PKI (infrastruktury veřejného klíče) vytvářet hierarchicky uspořádané struktury (stromy), s kořenovými autoritami v kořenech takovýchto stromů. Proto se u tohoto řešení hovoří o **stromu důvěry** (resp. v množném čísle „stromech důvěry“).

1.13.1 Pavučina důvěry, místo stromu důvěry

Alternativou ke „stromu důvěry“ může být **pavučina důvěry** (anglicky **web of trust**). Konkrétně řešení, v rámci kterého neexistují certifikační autority, které by uživatelům vydávaly jejich certifikáty – a místo toho si jednotliví uživatelé vydávají své certifikáty sami.[15]

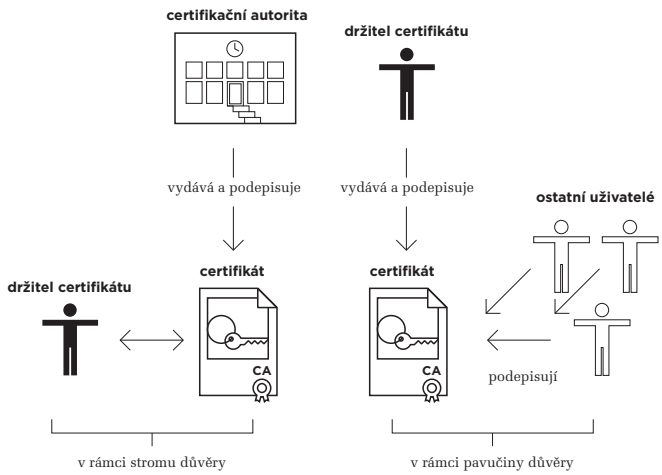
Jak je ale potom posuzována důvěryhodnost takovýchto certifikátů?

Základní princip je vcelku jednoduchý: důvěru v certifikát, vydaný samotným uživatelem, vyjadřují další uživatelé. Pokud daného uživatele znají, nejlépe osobně, mohou vyjádřit důvěru jeho certifikátu tím, že ho sami podepíší (opatří svým podpisem). Tím stvrzují, že oni důvěřují obsahu certifikátu. Tedy tomu, že veřejný klíč, obsažený v certifikátu, skutečně patří té osobě, jejíž identita je v certifikátu uvedena.

Svým způsobem tak tito další uživatelé nahrazují roli certifikační autority. Jestliže v rámci „stromu důvěry" certifikát podepisuje ta certifikační autorita, která jej vydává (a certifikát je tak podepsán pouze jednou), v rámci nyní popisované alternativy může být jeden certifikát podepsán apriorně neomezeným počtem dalších uživatelů.

Navíc to, že někdo podepíše certifikát jiného uživatele, může mít různý význam: může tím dávat najevo, že příslušného uživatele dobře zná a jeho certifikátu plně důvěřuje. Ale stejně tak může dát najevo to, že dotyčného zná „jen málo", a že jeho certifikátu důvěřuje „částečně".

Obrázek 1-27
Představa vydávání certifikátů v rámci stromu důvěry a v rámci pavučiny důvěry



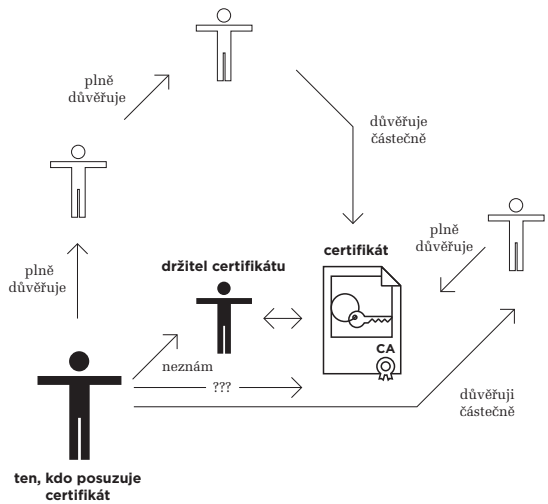
Jinými slovy: i zde je zásadní odlišnost oproti stromu důvěry, kde podpis certifikační autority na jí vydaném certifikátu má jen jeden možný význam (ve smyslu „plné důvěry"). Z pohledu toho, kdo s certifikátem pracuje, má pak důvěryhodnost absolutní charakter: certifikát pro něj buďto je důvěryhodný, nebo je nedůvěryhodný (případně jeho důvěryhodnost není schopen posoudit). Ale neexistuje zde něco jako: „tento certifikát je důvěryhodný na 50%".

15 A sami si je také podepisují. Jde tedy o certifikáty tzv. s vlastním podpisem (self signed), jak se dozvíme v dalších kapitolách.

V rámci pavučiny důvěry to ale možné je. Zde může být míra důvěry, udělovaná konkrétnímu certifikátu ostatními uživateli, různě odstupňována. Je pak na tom, kdo s takovýmto certifikátem pracuje, aby sám vyhodnotil, zda a do jaké míry mu bude důvěřovat. Aby jakoby „sečetl“ míru důvěry, kterou jiní uživatelé certifikátu vyjádřili, a na základě toho posoudil, zda výsledek již překročil hranici, kterou si sám zvolil – a za kterou již posuzovanému certifikátu bude důvěřovat i on.

Přitom všem ale musí dotyčný zohlednit i to, zda (a do jaké míry) sám důvěřuje těm uživatelům, jejichž názor na důvěryhodnost posuzovaného certifikátu právě využívá. Což je o to komplikovanější, že nemusí jít o přímý, ale pouze o zprostředkovaný vztah, ve smyslu: „znám a do určité míry důvěřuji někomu, kdo zná a do určité míry důvěřuje někomu jinému, kdo do takové a takové míry důvěřuje posuzovanému certifikátu“, viz obrázek.

Obrázek 1-28
Představa hodnocení důvěryhodnosti certifikátu v rámci pavučiny důvěry



Právě proto se zde hovoří o „pavučině důvěry“ – protože zde vzniká často dosti složité předivo vzájemných vztahů a vazeb důvěry mezi různými lidmi.[16]

1.13.2 Biometrické podpisy

Mnohem „odlišnější“ alternativou k elektronickým podpisům, popisovaným v této knize (a založeným na konceptu PKI, resp. stromech důvěry), mohou být tzv. **biometrické podpisy**. Jak už jejich název naznačuje, nějakým způsobem využívají biometrické charakteristiky podepisující osoby.

V širším slova smyslu může být biometrický podpis založen na jakékoli biometrické charakteristice. Tedy například na otisku prstu, vzorku sítnice atd.

V užším slova smyslu pak jsou biometrické podpisy založeny na tom, jak konkrétní člověk vytváří svůj klasický (vlastnoruční) podpis. Tedy nejenom na tom, jak samotný podpis vypadá (jako čárový obrázek), ale také na tom, jak byl vytvořen – jak rychle podepisující osoba pohybovala rukou, jaký tlak na podložku přitom vyvíjela atd.

Takovéto biometrické charakteristiky se dnes dají poměrně jednoduše nasnímat (pokud se člověk podepisuje speciálním perem na speciální podložku), převést do podoby dat a následně vyhodnocovat, spolu se samotným tvarem výsledného podpisu. Výsledek by totiž měl být skutečně unikátní, specifický pro každého jednotlivce a nenapodobitelný někým jiným.

Nelze ovšem nevidět, že takovéto biometrické podpisy mají některé zásadní odlišnosti oproti zde popisovaným elektronickým podpisům. Například by neměly být závislé na výpočetní síle počítačů, a díky tomu by mohly mít delší (apriorně neomezenou) platnost v čase. Na druhou stranu ale musí nějakým způsobem reagovat na lidské stárnutí a jím vyvolanou změnu biometrických charakteristik.[17]

Jinou principiální odlišností oproti elektronickým podpisům je to, že biometrické podpisy vyžadují něco jako „podpisové vzory“, pro potřeby svého ověřování (podobně, jako klasické vlastnoruční podpisy). A jejich správa (uchovávání, distribuce, i využití) může být netriviální záležitostí.

Zajímavou odlišností je také to, že biometrický podpis (na rozdíl od elektronického) může existovat sám o sobě a být nezávislý na tom, co je s ním podepsáno. Pak je ale problematické takové zajištění integrity podepsaného dokumentu, jaké očekáváme od dnes používaného elektronického podpisu. Nehledě již na takové aspekty, jako je neexistence biometrické alternativy pro elektronické značky, vytvářené stroji (programy). Jakýkoli elektronický dokument by pomocí biometrického podpisu musel (fyzicky) podepisovat konkrétní člověk. To by ale znemožňovalo použití tohoto druhu podpisu u takových služeb, které fungují plně automaticky.

Například provozovatel informačního systému datových schránek (ISDS) by musel zaměstnat řadu osob, které by svým jménem podepisovaly jednotlivé datové zprávy (zatímco dnes jsou podepisovány strojově, bez lidského zásahu – a také bez toho, že by se někdo s jejich obsahem seznamoval).

---

16 V praxi je řešení na principu pavučiny důvěry používáno zejména v rámci systémů PGP (Pretty Good Privacy).

17 Proto se někdy hovoří i o dynamických biometrických podpisech, které se snaží brát tyto změny v úvahu.

Úroveň II – Principy

2. Vytváření elektronických podpisů

Kapitola 2

2. Vytváření elektronických podpisů

V této kapitole si již podrobněji popíšeme podstatu elektronických podpisů, ale i značek a časových razítek. Zajímat nás bude hlavně způsob jejich vzniku, zatímco problematiku jejich ověřování (vyhodnocování jejich platnosti) si necháme na další samostatnou kapitolu.

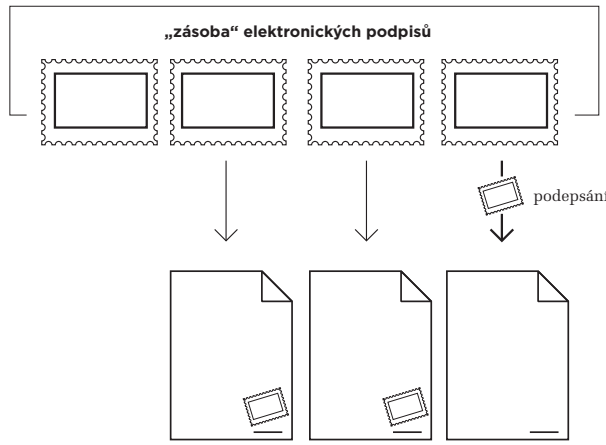
Stejně tak se ještě nedostaneme k otázkám právním, ty si necháme na samostatnou kapitolu. I když určité prvky práva nám proniknou i sem, alespoň pokud jde o terminologii: když už se budeme o něčem bavit po věcné stránce, naznačíme si současně, jak se tomuříká ve světě zákonů a vyhlášek. Protože tam se věcem často říká úplně jinak, než v běžné praxi.

2.1 Elektronický podpis není jako známka

V zájmu co nejlepší srozumitelnosti začneme v cimrmanovském duchu neboli prozkoumáním slepých uliček. Konkrétně popisem toho, čím elektronický podpis není. Nebo ještě přesněji: jaké jsou nesprávné pohledy na tu variantu elektronického podpisu, kterou se zabýváme v této knize, a která je založena na asymetrické kryptografii a na infrastruktuře veřejného klíče.[1]

Snad nám tyto protipříklady umožní lépe pochopit, čím elektronický podpis doopravdy je a jaké má vlastnosti. Jedním z „alternativních“ pohledů by mohla být představa, že elektronický podpis je něčím jako známkou či kolkem.

Obrázek 2-1
Představa elektronického podpisu jako známky



[1] Na rozdíl od závěru předchozí kapitoly nám zde již nejde o „jiné elektronické podpisy“, neboli o alternativy k tomu elektronickému podpisu, který je zakotven v našem právním řádu a kterému je věnována celá tato kniha. Zde jde o jiné pohledy na tento jeden konkrétní druh podpisu.

Pokud by tomu tak bylo, pak by elektronický podpis mohl existovat „sám o sobě“ a nezávisle na tom, co s ním bude podepsáno. Díky tomu by se dal vytvořit i nějak dopředu, jakoby „do zásoby“ (stejně, jako se dopředu dají tisknout známky či kolky) – a teprve následně, v okamžiku skutečné potřeby, by se nějak připojil („nalepil“) ke konkrétnímu dokumentu, v roli jeho podpisu.

Takováto představa by stále mohla zajistit to, aby elektronický podpis byl spojen s konkrétní osobou – pokud by „známky v roli podpisů“ byly vytvářeny jako individuální (vztažené ke konkrétní osobě), a nikoli jako klasické známky, které jsou vždy stejné a nezávislé na tom, kdo si je koupí a na něco nalepí. Jinými slovy: každý by potřeboval své vlastní a individuální „elektronické podpisy jako známky“.

Co by ale už splněno nebylo, je požadavek na to, aby elektronický podpis umožnil detekovat jakoukoli změnu podepsaného dokumentu (neboli: porušenou integritu). To by zde nešlo, kvůli tomu, že „elektronický podpis jako známka“ by byl zcela nezávislý na tom, co jím je podepsáno.

Konkrétním příkladem „elektronického podpisu jako známky“ by mohlo být naskenování něčího vlastnoručního podpisu do podoby obrázku (analogie vytvoření „známky“), a přidání tohoto obrázku ke konkrétnímu textu v elektronické podobě, nejspíše v textovém editoru (jako analogie nalepení známky). Příklad s již jednou zmiňovaným podpisem prezidenta republiky naznačují obrázky.

Obrázek 2-2
Vyobrazení podpisu Václava Klause

Obrázek 2-3
Text s přiloženým snímkem podpisu Václava Klause

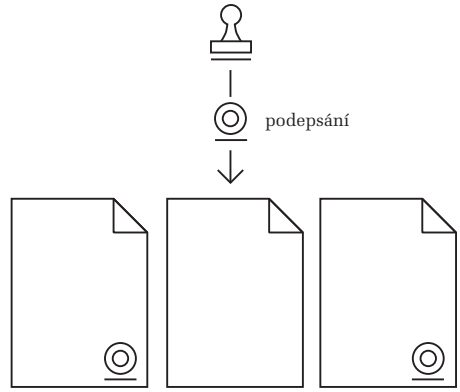
Právníci by vůči takovémuto postupu určitě namítali, že zde chybí projev vlastní vůle: svůj podpis k textu v rámci tohoto příkladu opravdu nepřipojil Václav Klaus, aby tím vyjádřil svůj souhlas s uvedeným textem.

Představu elektronického podpisu „jako známky" tedy musíme odmítnout.[2]

2.2 Elektronický podpis není jako otisk razítka

Dalším „alternativním" pohledem na podstatu elektronického podpisu by mohla být představa, že jde o jakousi obdobu otisku razítka.

Obrázek 2-4
Představa elektronického podpisu jako razítka



[2] Zajímavé je, že první návrh zákona o elektronickém podpisu z roku 1999, který byl v ČR představen veřejnosti, byl založen právě na tomto pohledu. Místo o podepisující či podepsané osobě hovořil o „oprávněné osobě" (oprávněné nakládat s vlastním elektronickým podpisem), a ukládal jí povinnost „nakládat s elektronickým podpisem s náležitou péči tak, aby nemohlo dojít k jeho neoprávněnému použití".

Při této představě by už elektronický podpis nemohl existovat „sám o sobě“ a nemohl by vznikat „dopředu“. Tedy pokud si odmyslíme elektronickou obdobu orazítkování prázdného listu papíru, na který teprve následně někdo něco napíše.

Důležité ale je, že i takovýto „elektronický podpis jako otisk razítka“ by byl vždy stále stejný a tudíž nezávislý na tom, co a jak je jím podepisováno. Takže by stále nebyl splněn požadavek, aby elektronický podpis umožňoval detekovat jakoukoli změnu toho, co je podepsáno (tj. porušenou integritu).

Než ale odmítneme i tuto představu o elektronickém podpisu, řekněme si o jedné její přednosti (alespoň oproti předchozí představě „elektronického podpisu jako známky“). Jde o samotné razítko, které by samozřejmě už nebylo označováno jako razítko, ale nejspíše jako „prostředek“, konkrétně jako **prostředek pro vytváření elektronických podpisů**. Tedy alespoň v řeči práva a právních předpisů.

Aby mohl být splněn požadavek na jednoznačné určení toho, kdo podpis vytvořil (resp. kdo se podepsal), musel by i tento prostředek být individuální: každá osoba, která by se elektronicky podepisovala, by musela mít vlastní prostředek pro vytváření elektronických podpisů. A jistě není těžké si domyslet, že by takovýto prostředek musela držet pod svou kontrolou (tj. nedávat z ruky), aby se jejím jménem nemohl podepisovat někdo jiný. Stejně, jako se musí „držet pod kontrolou“ i nejrůznější kulatá razítka.

2.3 Prostředky a data pro vytváření elektronických podpisů

Než definitivně zavrhneme představu elektronického podpisu jako otisku razítka, zastavme se ještě na chvíli u jiného problému této představy. Pokud bychom ji chtěli uvést do života, pak by „prostředek pro vytváření elektronických podpisů“ nutně musel mít elektronickou podobu: musel by to být nějaký program, pomocí kterého bychom svůj elektronický podpis vytvářeli.

Jelikož by ale tento „prostředek“ ve formě programu musel být individuální (aby jeho aplikací vznikal „náš“ vlastní podpis, a nikoli nějaký univerzální podpis), musel by i celý tento program být individuální, šitý na míru konkrétní fyzické osobě.

To by samozřejmě bylo možné a realizovatelné, ale bylo by to velmi nepraktické. Nemohl by to být běžný program, který bychom si mohli kupovat „jako housku na krámě“ (jako nějaký hotový produkt), ale museli bychom si ho nechat vytvářet na míru. To by bylo velmi drahé, a drahá by byla také jeho individuální distribuce. Nemluvě již o používání takového programu, který by musel být instalován nějak specificky (tak, aby se k němu nedostali ostatní uživatelé téhož počítače), musel by být chráněn proti kopírování atd.

Naštěstí ale má celý tento problém poměrně jednoduché řešení: nebudeme pracovat s jedním „celistvým“ prostředkem pro vytváření elektronických podpisů, ale rozdělíme ho na dvě části:

- na část „univerzální“, která bude moci být pro všechny uživatele stejná
- na část „individuální“, která již bude specifická pro každého konkrétního uživatele.

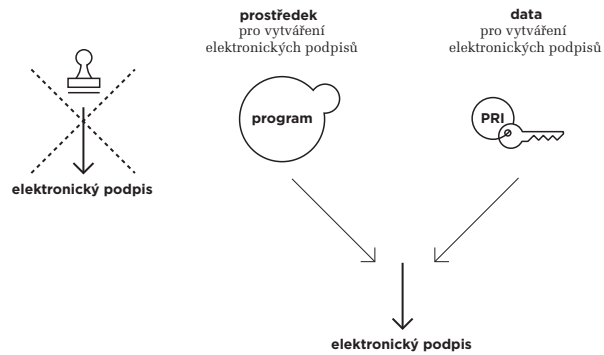
Výhodou bude to, že roli „univerzální části“ pak již budeme moci svěřit programu, který bude jeden, resp. bude stejný pro všechny uživatele – a jeho výroba, distribuce i instalace a používání se tím významně zjednoduší i zlevní. A nebude ani nutné tento program nějak specificky chránit proti zcizení či zkopírování, aby se nedostal do rukou někomu jinému.[3]

Takováto ochrana bude nadále nutná jen u „individuální“ části. Pokud se ale celé rozdělení provede šikovně, může být tato individuální část dostatečně malá a taková, aby se s ní dalo snáze (a levněji) nakládat tak, aby bylo učiněno zadost všem požadavkům na ochranu a bezpečnost.

Pokud jde o terminologii, asi již tušíte, že onou „individuální částí“ je v praxi **klíč**, konkrétně **soukromý klíč** (resp. **privátní klíč**), využívaný při tvorbě (zaručeného) elektronického podpisu. Zákon o elektronickém podpisu o něm ale nehovoří jako o klíči, ale jako o „datech“. Místo o soukromém klíči tak hovoří o **datech pro vytváření elektronických podpisů**.

No a „univerzální část“ si podržela označení původního celku (razítka) – a tak právě ona je **prostředkem** (konkrétně: **prostředkem pro vytváření elektronického podpisu**). Tak ji definuje i zákon o elektronickém podpisu.

Obrázek 2-5
Představa elektronického podpisu, vzniklého aplikací dvou složek



Zopakujme si tedy celkovou představu, kterou bychom mohli označit jako představu „dvousložkového“ elektronického podpisu. Ten vzniká aplikací dvou složek:

- (univerzálního) **prostředku** pro vytváření elektronických podpisů, a
- (individuálních) **dat** pro vytváření elektronických podpisů (tj. soukromého klíče)

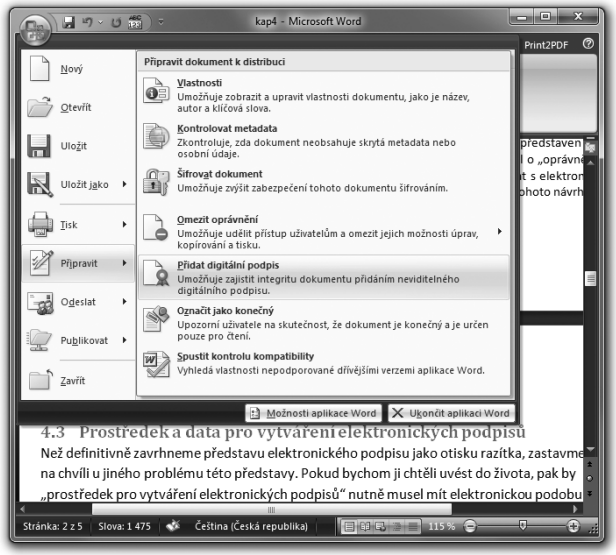
Doplňme si ještě jeden zajímavý postřeh: prostředek pro vytváření elektronických podpisů nemusí mít pouze formu jednoúčelového programu, který slouží právě a pouze k (elektronickému) podepisování.

[3] Toto je samozřejmě myšleno pouze ve smyslu ochrany osobních údajů, nikoli ve smyslu možnosti volného šíření komerčních programů chráněných licenčními podmínkami.

Stejně tak dobře může jít o jednu z funkcí nějakého programu, který primárně slouží k jiným účelům.

Příkladem mohou být různé kancelářské balíky (jako je MS Office apod.), určené pro běžnou práci s dokumenty. Kromě toho ale mají schopnost tyto dokumenty také elektronicky podepisovat (byť samy mohou hovořit o digitálních podpisech, místo podpisech elektronických).

Obrázek 2-6
Možnost přidání elektronického (digitálního) podpisu v editoru MS Word z balíku MS Office 2007



2.4 Zajištění integrity podepsaného dokumentu

Představa elektronického podpisu, kterou jsme si vykreslili v předchozí části této kapitoly, je už relativně blízko k realitě. Stále jí ale chybí jedna podstatná věc, a tou je schopnost „dvousložkového“ elektronického podpisu zajistit integritu dokumentu. Nikoli ve smyslu zabránění jakýmkoli změnám, ale jako možnost spolehlivě rozpoznat, pokud by k nějaké změně došlo.

Pokud by elektronický podpis skutečně vznikal výše popsaným způsobem, tedy jen jako „dvousložkový“ (kombinující pouze prostředek a data pro vytváření elektronických podpisů), byl by stále nezávislý na tom, co je podepisováno. Takový podpis by stále mohl existovat „sám o sobě“, a bylo by možné si ho vytvořit nějak „dopředu“, resp. „do zásoby“. Pak by ale skutečně nemohl zajišťovat integritu (neporušenost) toho dokumentu, který jím bude podepsán.

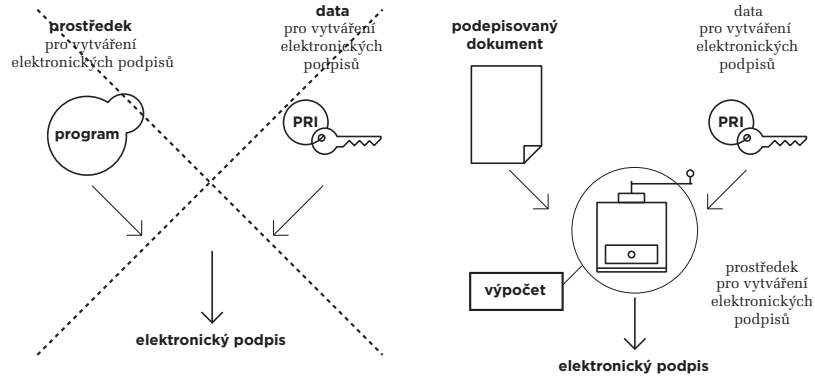
Má-li elektronický podpis zajišťovat integritu podepsaného dokumentu, musí být na tomto dokumentu nějakým způsobem závislý. Musí určitou formou odrážet jeho obsah – aby při sebemenší změně tohoto obsahu již podpis „neseděl“ (neodrážel korektně jeho obsah).

Aniž bychom museli zacházet do detailů, připomeňme si, že elektronický podpis je ve své podstatě číslem, a že vytvoření elektronického podpisu je vlastně vypočítáním tohoto čísla. My nyní chceme, aby při sebemenší změně již podepsaného dokumentu původně vypočítané číslo (podpis) již nesedělo, resp. aby pro pozměněný dokument vycházelo (jako jeho elektronický podpis) už jiné číslo.

Toho dosáhneme tak, že výpočet čísla v roli elektronického podpisu bude vhodným způsobem vycházet i z obsahu podepisovaného dokumentu.

Musíme si tedy znovu upřesnit naši představu o vzniku elektronického podpisu: musí jít o výpočet, který provádí „prostředek pro vytváření elektronických podpisů“, a jeho vstupem (tj. daty na jeho vstupu, které jsou při výpočtu zpracovávány) bude jak soukromý klíč (data pro vytváření elektronických podpisů), tak i samotný podepisovaný dokument. Představu ilustruje obrázek.

Obrázek 2-7
Představa závislosti podpisu na podepsaném dokumentu



Zdůrazněme si nyní důsledky, které z právě naznačeného způsobu vzniku elektronického podpisu vyplývají:

- dosáhli jsme požadovaného efektu, potřebného pro zajištění integrity podepsaného dokumentu: pokud by došlo k sebemenší změně již jednou podepsaného dokumentu, ihned bychom to poznali. Konkrétní způsob výpočtu elektronického podpisu, na obrázku naznačený „kafemlýnkem“, totiž musí být volen tak, aby při skutečně sebemenší změně dokumentu (například v jednom jediném bitu) skutečně vycházel elektronický podpis jinak (jako jiné číslo).
- ještě dalším důležitým důsledkem je to, že nyní již elektronický podpis z principu nemůže existovat „sám o sobě“ a nezávisle na podepsaném dokumentu. Nejde ho vypočítat nějak „dopředu“, nezávisle na tom, co je podepisováno (na dokumentu).

Jiným, neméně zajímavým důsledkem by mělo být to, že různé dokumenty budou vždy mít různý podpis. Tedy: až na tzv. kolizní dokumenty, které jsou jiné (než daný dokument), ale mají stejnou hodnotu podpisu (jako daný dokument). A to je věc, která si také zaslouží podrobnější vysvětlení.

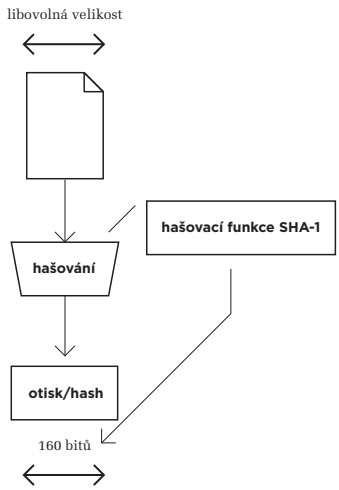
2.5 Hašování a hašovací funkce

Abychom si mohli vysvětlit, co jsou kolizní dokumenty, musíme si znovu poopravit naši představu o vzniku elektronického podpisu, a to zmínkou o tzv. **hašování** (anglicky: **hashing**) a **hašovacích funkcích**.

V češtině bychom mohli hovořit také o vytváření **otisků**, ale sloveso „otiskování“ by nebylo až tak přirozené. A tak se raději podržíme oficiálního termínu **hašování.**

Podstatu hašování si můžeme zjednodušeně představit jako inteligentní zmenšování. Jako vytvoření „něčeho menšího z něčeho většího“.

Obrázek 2-8
Představa hašování (s hašovací funkcí SHA-1)



Důvodem pro potřebu hašování je to, že při podepisování (ale i při označování, neboli při vytváření elektronických značek, stejně jako při vytváření časových razítek, při šifrování apod.) potřebujeme pracovat s bloky dat o pevné velikosti. Metody a algoritmy, které se k podepisování používají, to zkrátka vyžadují. Navíc je vhodné i to, aby ony bloky pevné velikosti byly dostatečně malé. „Dostatečně“ na to, aby jejich zpracování (nejen v rámci elektronického podepisování, ale třeba i šifrování), mohlo být dostatečně rychlé.

> Ještě v roce 2009 se i v oblasti elektronického podpisu nejčastěji používala hašovací funkce **SHA-1**. Ta vytváří otisky (hash-e) o velikosti 160 bitů. Jinými slovy: z podepisovaného dokumentu, který mohl mít například několik megabytů, se hašováním nejprve vytvoří otisk (hash) o velikosti 160 bitů (a teprve ten se pak podepisuje).

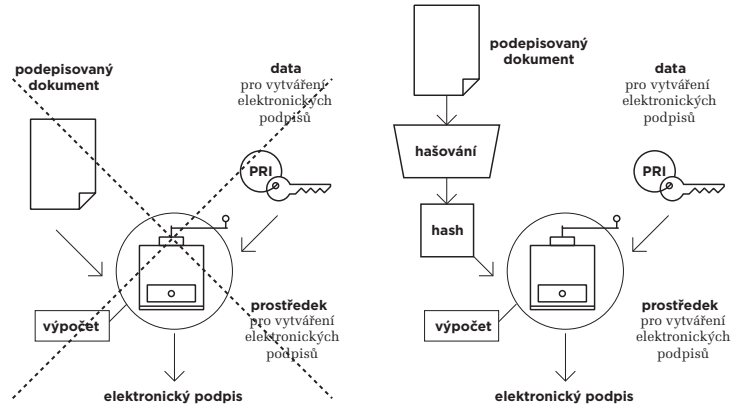
> Od počátku roku 2010 je doporučeno používat propracovanější hašovací funkce z rodiny **SHA-2**, které již pracují s většími otisky: velikosti 224, 256, 384, nebo 512 bitů.

Na druhou stranu jako uživatelé chceme mít možnost podepisovat libovolně velké dokumenty. Takže hašování, coby převodu z „libovolně velkého“ na „pevně danou velikost“ (či spíše „pevně danou malost“), se tak jako tak nevyhneme.

Naštěstí je ale vše zařízeno tak, abychom se jako uživatelé při podepisování nemuseli o nic starat a mohli podepisovat skutečně libovolně velké dokumenty. Potřebné hašování je totiž zabudováno do procesu vzniku elektronického podpisu.

To ale znamená, že si opět musíme poněkud poupravit naši představu toho, jak elektronický podpis vlastně vzniká: nejprve je z podepisovaného dokumentu vytvořen jeho otisk (hash), a teprve ten je pak podepsán. Představu opět ukazuje obrázek.

Obrázek 2-9
Představa hašování při vytváření elektronického podpisu



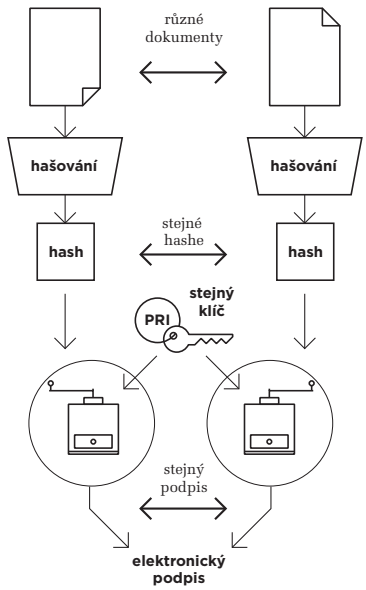
2.5.1 Máme se bát kolizí?

Používání hašování a hašovacích funkcí na jedné straně řeší problém s podepisováním libovolně velkých dokumentů, na druhé straně ale vytváří jiný nepříjemný problém. Jeho podstata vyplývá již ze samotného principu hašování, kdy se „z něčeho většího“ stává „něco menšího“: budou existovat takové dokumenty, které sice budou navzájem odlišné, ale jejich „zmenšeniny“ (otisky, hash-e) budou stejné.

Jenže: když se při podpisu z takto různých dokumentů nejprve udělají jejich otisky (které vyjdou stejné), a tyto otisky se následně podepíší, vznikne z toho stejný elektronický podpis (ve smyslu: se stejnou hodnotou, chápeme-li jej jako číslo).

Jinými slovy: budeme mít dva různé dokumenty, ale jeden elektronický podpis. A už nebudeme schopni rozlišit, zda tento podpis „patří“ jednomu či druhému dokumentu. Správně totiž „patří“ oběma.

Obrázek 2-10
Představa kolizních dokumentů



Došlo by tedy k něčemu, co bychom mohli označit jako **kolizi** (dvou dokumentů s jediným otiskem) – a podle toho se také takovéto dokumenty označují jako **kolizní dokumenty.**[4]

Samozřejmě je to nežádoucí situace, které bychom se měli vyhnout. Protože když by nám někdo předložil nějaký elektronicky podepsaný dokument, jak bychom se ujistili, že je to skutečně ten původně podepsaný a nikoli nějaký jiný (a to kolizní) dokument? Ze samotného ověření elektronického podpisu bychom to nepoznali, protože to by změnu dokumentu (skrze porušení jeho integrity) neodhalilo.

Existenci kolizních dokumentů ale nemůžeme v principu zabránit. Jak jsme si již uvedli, vyplývá už ze samotné podstaty hašování, kdy „něco většího“ zmenšujeme na „něco menšího“.[5]

Musíme se tedy smířit s tím, že kolizní dokumenty existují.[6] Jak ale potom může vůbec fungovat elektronický podpis a jak mu můžeme důvěřovat, když z principu nelze vyloučit existenci kolizních dokumentů? Odpověď na tuto velmi zajímavou otázku je sama o sobě nesmírně důležitá a má velmi závažné důsledky, zejména pokud jde o dlouhodobou platnost elektronických podpisů. Jak ale tato odpověď zní?

4 V praxi bychom ještě měli rozlišovat mezi **kolizemi prvního** a **druhého řádu**. Kolizí prvního řádu se rozumí nalezení (jakýchkoli) dvou dokumentů, které mají stejný otisk (hash). To by mělo být jednodušší než kolize druhého řádu, při které ke známému dokumentu hledáme druhý (odlišný) dokument se stejným otiskem.

5 Přesnější zdůvodnění je takové, že neexistuje prosté (injektivní) zobrazení z větší do menší množiny.

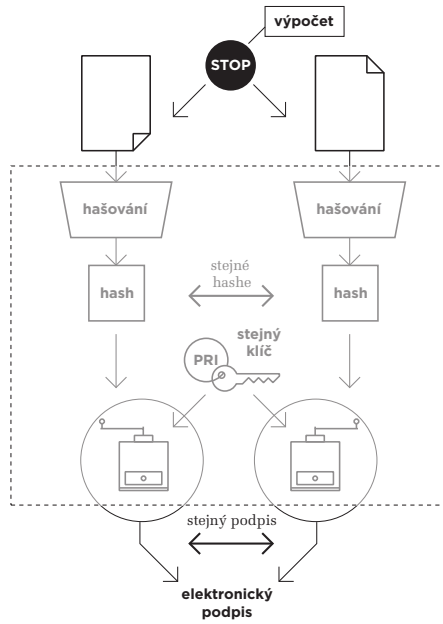
6 Ba co více: ke každému konkrétnímu dokumentu již z principu existuje nekonečně mnoho kolizních dokumentů.

Zní tak, že samotná existence kolizních dokumentů nám ještě vadit nemusí – pokud je zajištěno, že nikdo nebude reálně schopen nalézt (vypočítat) jakýkoli kolizní dokument v takovém čase, který by mu umožňoval nějaké reálné zneužití.

Jinými slovy: jde o to, aby hledání kolizních dokumentů (tj. jejich výpočet) bylo tak ztíženo, aby nešlo dělat příliš rychle. Aby příslušný výpočet byl tak složitý (výpočetně náročný), že zabere neúnosně dlouhou dobu a nejde ho zkrátit ani jakkoli „obejít". A ona „dlouhá doba" by neměla být kratší, než jsou nějaké stovky či lépe miliony let – aby se skutečně nikomu nevyplatilo čekat na výsledek.

K nemožnosti hledat kolizní dokumenty „nějak rychleji" patří i správná konstrukce hašovacích funkcí. Ty samozřejmě nemohou fungovat na nějakém „naivním" principu, tak aby je šlo obelstít a tím zrychlit hledání kolizí. Nebo dokonce nějak „obrátit", tak aby se z otisku dal odvodit původní dokument.

Obrázek 2-11
Představa nemožnosti výpočtu kolizního dokumentu



Správně navržená hašovací funkce musí například „reagovat" na jakoukoli změnu výchozího dokumentu: i kdyby se na něm změnil jen jeden jediný bit, musí být nový otisk odlišný od původního otisku. Ostatně, jinak by se nedala zajistit integrita dokumentu, kterou požadujeme od elektronického podpisu: pokud by při změně dokumentu zůstával jeho otisk beze změny, porušení integrity by se nedalo zjistit.

2.6 Faktor času u elektronického podpisu

Když víme, že kolizní dokumenty existují, a chceme-li co nejvíce ztížit jejich hledání (resp. výpočet), pak musíme počítat s tím, že to bude nekonečný boj, který nikdy nebude mít vítěze. To proto, že na jedné straně sice můžeme uměle zvyšovat náročnost hledání kolizních dokumentů tak, aby jejich výpočet nebyl kratší než nějaká opravdu hodně dlouhá doba, ale proti nám bude neustále (a velmi rychle) narůstat výpočetní síla našich počítačů. Tedy spíše výpočetní síla počítačů našich protivníků.

Takže pokud „nadimenzujeme“ nějaký výpočet tak, aby ho počítače z určité historické epochy nedokázaly provést v únosném čase (dříve než za nějaké ty miliony let, například), tak aby nehrozilo reálné zneužití pomocí nalezeného kolizního dokumentu, budoucí počítače si mohou poradit se stejným výpočtem v podstatně kratším čase, například již jen v řádu měsíců, týdnů, dnů apod. – a případné zneužití by již reálně hrozilo. Takže my zase musíme na své straně znovu zvýšit složitost celého výpočtu, nutného pro nalezení kolizního dokumentu.

Cestou k tomuto zvyšování výpočetní složitosti je především „zvětšování rozměrů“, konkrétně třeba zvyšování počtu bitů nejrůznějších klíčů, velikostí otisků (hash-ů) atd., a také používání stále silnějších a propracovanějších kryptografických algoritmů, hašovacích funkcí atd. Vedle toho ale musíme stále pamatovat i na to (a starat se o to), aby se případný výpočet kolizního dokumentu nemohl ubírat nějakou jinou (hlavně kratší) cestou, než tou, kterou takto uměle prodlužujeme.

Navíc musíme veškeré „průběžné posilování“ realizovat s dostatečným předstihem, protože odhadovat růst schopností naší výpočetní techniky je velmi obtížné – a čekat na situaci „až k tomu dojde“ by bylo fatální, protože to bychom už mohli mít v oběhu reálně nalezené kolizní dokumenty, bez možnosti jejich přímého odlišení od dokumentů původních (pravých).

> V roce 2010 došlo právě k jednomu průběžnému posílení, konkrétně u hašování: původně používaná hašovací funkce SHA-1 byla nahrazena „silnější“ hašovací funkcí SHA-2 (resp. celou rodinou takovýchto hašovacích funkcí). Všechny tři akreditované certifikační autority od tohoto data také přestaly vydávat své kvalifikované certifikáty s původní hašovací funkcí SHA-1, a nově vydávají kvalifikované certifikáty již jen s některou z hašovacích funkcí SHA-2. Stejně tak došlo ke zvětšení používaných klíčů, minimálně na 2048 bitů.

2.6.1 Proč elektronické podpisy zastarávají?

Průběžné posilování dat i prostředků pro vytváření elektronických podpisů je samozřejmě v praxi realizovatelné, a také se realizuje (pro nově vytvářené podpisy). Jenže to nestačí: co s těmi elektronickými podpisy (a stejně tak značkami i razítky), které již byly vytvořeny?

U těch už žádné průběžné posilování není možné, protože je nelze jakkoli (ani zpětně) měnit. A tak se vše musí řešit na jiném principu: časovým omezením. Nikoli ale tak, že by se konstatovalo, že jednou vytvořený elektronický podpis (či značka nebo razítko) po určitém čase přestává platit. To by nešlo

už z právních důvodů: podepsání, resp. připojení podpisu – ať již vlastnoručního či elektronického – je právním úkonem, jehož důsledky nejsou apriorně omezovány v čase. Pokud by měly být, znamenalo by to například, že by nešlo uzavírat smluvní vztahy elektronickou cestou na dobu delší, než je toto časové omezení.

Proto se „časové omezení" aplikuje jinde: nikoli na platnosti podpisu jako takového, ale na možnosti ověřit tuto platnost. Ta je záměrně nastavena jen na dobu určitou, která je navíc volena tak, aby zcela určitě (a spíše s dostatečnou rezervou) skončila dříve, než bude reálně možné vypočítat nějaký kolizní dokument.

V praxi to konkrétně znamená, že se uměle omezuje „životnost" (doba platnosti) certifikátů, na kterých jsou konkrétní podpisy (či značky nebo razítka) založeny: po uplynutí této jejich platnosti již není možné se spoléhat na informace, které tyto certifikáty stvrzují.

> Konkrétně u certifikátů, na kterých jsou založeny elektronické podpisy a elektronické značky, je jejich řádná platnost obvykle nastavena na 1 rok.[7] V případě certifikátů, na kterých jsou založena časová razítka, bývá jejich platnost delší (u certifikátů od CA PostSignum jde o 3 roky, od I. CA jde o 5 let, a od eIdentity na 6 let).

Problematikou platnosti elektronických podpisů v dlouhodobějším časovém horizontu se teprve budeme podrobněji zabývat (ve čtvrté kapitole, v části 4.10). Proto si jen zdůrazněme základní princip:

Platnost elektronického podpisu jako takového není v čase apriorně omezována. Omezována je možnost ověřit (a tím i prokázat) platnost podpisu s využitím certifikátu, na kterém je podpis založen, a to skrze umělé omezení životnosti tohoto certifikátu.

Možnost prokázat platnost podpisu a pravost podepsaných dokumentů v delším časovém horizontu se tím neuzavírá – jen musí být realizována jinak.

2.6.2 Doba vzniku elektronického podpisu

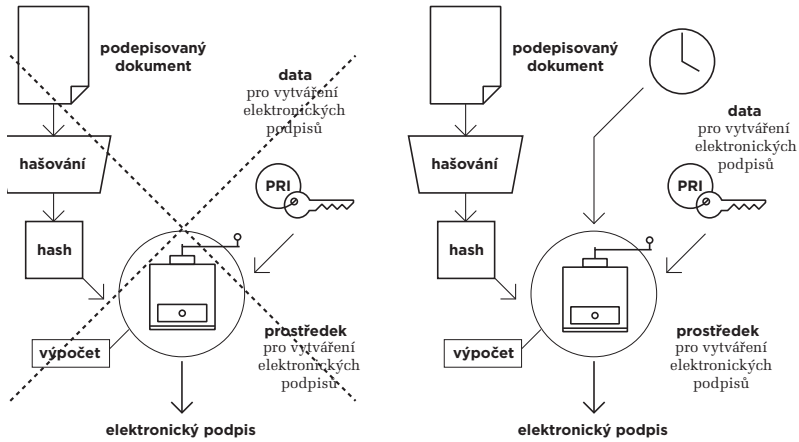
Celá věc kolem ověřování (vyhodnocování platnosti) elektronického podpisu je ale ještě komplikovanější a nejde v ní jen o aktuální platnost či neplatnost příslušného certifikátu. Jde také o to, kdy přesně konkrétní elektronický podpis (či značka) vznikl – a zda v této době byl certifikát platný. Obecně totiž musíme posuzovat platnost elektronického podpisu k okamžiku jeho vzniku.

Jak ale zjistíme, kdy konkrétní elektronický podpis vznikl? Odpověď by na první pohled mohla být triviální: každý elektronický podpis (i značka) v sobě obsahuje údaj o době svého vzniku.

---

[7] Alespoň u certifikátů od tuzemských certifikačních autorit. V zahraničí se lze setkat i s delší platností.

Obrázek 2-12
Upřesněná představa vzniku el. podpisu, se zahrnutím časového údaje



Dokonce si tedy musíme znovu poupravit naši průběžně budovanou představu toho, jak elektronický podpis vlastně vzniká: kromě otisku podepisovaného dokumentu a soukromého klíče (dat pro vytváření elektronického podpisu) do něj vstupuje ještě údaj o čase, kdy podpis vzniká.

Problém je ale v tom, že tento údaj o čase je přebírán ze systémových hodin počítače, na kterém elektronický podpis vzniká. S těmito systémovými hodinami však může uživatel počítače manipulovat a nastavit si na nich takový čas, jaký potřebuje. A ten se pak vloží i do elektronického podpisu jako údaj o přesném okamžiku jeho vzniku.

Jinými slovy: elektronický podpis sice obsahuje nějaký údaj o čase, ale na ten se nemůžeme spoléhat. Takže je to vlastně stejné, jako kdyby tam vůbec nebyl. A to znamená, že vlastně nikdy nevíme (dostatečně spolehlivě), kdy přesně ten který elektronický podpis vznikl.[8]

2.7 Časová razítka

Problém s nedůvěryhodností časového údaje „uvnitř“ elektronického podpisu je samozřejmě řešitelný: údaj o čase si necháme poskytnout od nějaké dostatečně důvěryhodné třetí strany. Od někoho, kdo má přímo povinnost mít správně seřízené hodinky, a bude také ručit za správnost poskytnutého časového údaje.

Jenže opět narazíme na další problém: jak zajistit, aby byl tento důvěryhodný časový údaj skutečně použit a „vložen“ do vznikajícího elektronického podpisu, a nebyl zde žádný prostor pro nějakou manipulaci a změnu časového údaje. To už je mnohem těžší – ale i to se dá ošetřit. Princip je takový, že důvěryhod-

ný časový údaj se nebude vkládat do samotného podpisu (podepisující osoby), ale bude vložen do jiného (dalšího) podpisu, který vytvoří přímo ten, kdo důvěryhodný časový údaj poskytuje.[9]

Jenže i zde je problém: tento „další podpis" nemůže být zákonem kvalifikován jako elektronický podpis (ani jako elektronická značka), protože postrádá jeho základní atributy. Především nepředstavuje žádné vyjádření souhlasu či jiného stanoviska k obsahu samotného dokumentu.

Proto se zde hovoří o **časovém razítku**, místo o elektronickém podpisu či značce. A to i v zákonech, kde je časové razítko definováno a má skutečně úplně jiné postavení, než elektronický podpis: pouze osvědčuje, že to, co je časovým razítkem opatřeno, již existovalo v době vzniku časového razítka. Přesněji, abychom dodrželi dikci zákona: existovalo před okamžikem, uvedeným na časovém razítku.

V praxi tedy budeme časové razítko používat k tomu, abychom „zafixovali" dobu vzniku elektronického podpisu: když budeme mít elektronický dokument, opatřený elektronickým podpisem, přidáme k němu ještě časové razítko. Tím „zafixujeme" (stvrdíme) to, že elektronický podpis na dokumentu již existoval (k okamžiku, uvedeném na časovém razítku), a tudíž musel vzniknout někdy dříve.

Zdůrazněme si, že časové razítko neříká, jak dlouho již existuje to, co je časovým razítkem právě opatřováno. Elektronický podpis na dokumentu, ke kterému je připojováno časové razítko, mohl vzniknout jen o zlomky sekund dříve, ale stejně tak mohl vzniknout o mnoho hodin, dnů, týdnů či roků dříve. To z časového razítka není patrné.

Pro „správný efekt" časového razítka je také nutné respektovat správné pořadí: má-li časové razítko stvrzovat existenci elektronického podpisu v čase, musí být k dokumentu připojeno AŽ PO elektronickém podpisu. Nikoli obráceně.[10]

Dalším důležitým aspektem časového razítka je to, že v zásadě jej může vytvořit kdokoli. Tedy třeba i ten, kdo se na nějaký dokument sám podepisuje. Takové časové razítko by ale neplnilo svůj účel, protože bychom se nemohli dostatečně spoléhat na správnost časového údaje, který je v časovém razítku obsažen.

Proto mají v praxi smysl jen taková časová razítka, která poskytují specializovaní poskytovatelé: **autority časových razítek**, v angličtině **TSA (Time Stamping Authority)**, jejichž činnost se řídí požadavky zákona. V terminologii našich zákonů jsou to **kvalifikovaní poskytovatelé certifikačních služeb, vydávající kvalifikovaná časová razítka**. Říkejme jim pro jednoduchost **poskytovatelé časových razítek.**

---

8 Tedy pokud nebudeme brát v úvahu nějaká zcela „jiná" řešení, jako například notářské osvědčení o tom, že podpis byl vytvořen před notářem v takový a takový okamžik.

9 Z tohoto principu se ale vymyká koncepce (interních) časových razítek u PDF dokumentů, kde časové razítko není samostatné, ale garantovaný údaj o čase je vkládán přímo do samotného elektronického podpisu. Podrobněji viz část 6.3.

10 „Obráceně" je časové razítko aplikováno u datových zpráv, které prochází skrze informační systém datových schránek.

> V roce 2010 působili v ČR tři poskytovatelé časových razítek, splňující požadavky zákona (kvalifikovaní poskytovatelé, vydávající kvalifikovaná razítka): společnosti I.CA, PostSignum a eIdentity.

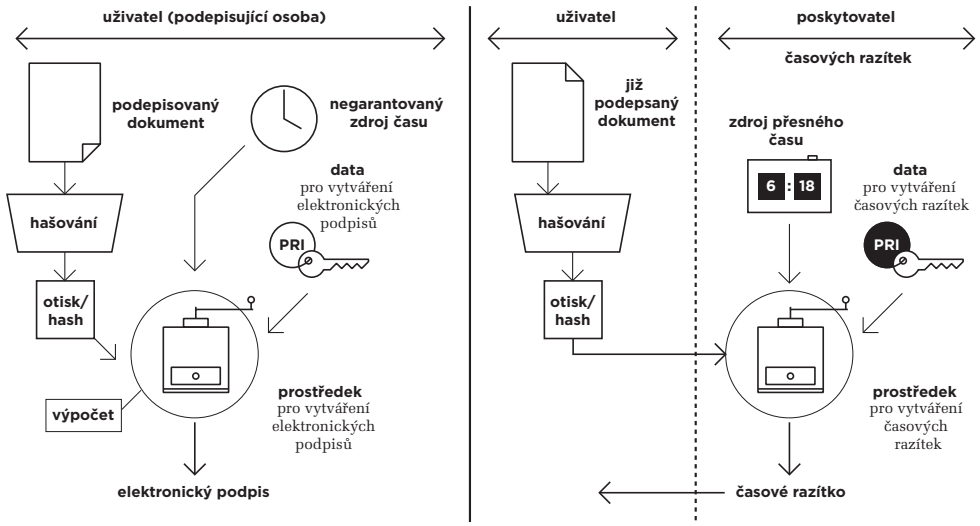
2.7.1 Jak vzniká časové razítko?

Pro správné pochopení a docenění časových razítek si ještě popišme, jak vlastně vznikají. Způsob jejich vzniku je principiálně shodný s tím, jak vznikají elektronické podpisy. Liší se ale to, kdo provádí jednotlivé úkony. Sledujme to i na následujícím obrázku:

- z dokumentu, který má být opatřen časovým razítkem, se nejprve vytvoří otisk (hash) pevné velikosti. K tomu dochází „u uživatele", a tedy úplně stejně, jako u elektronického podpisu
- v dalším kroku je otisk odeslán poskytovateli časových razítek, a ten jej podepíše s využitím svého soukromého klíče.[11] Výsledek již představuje samotné časové razítko jako takové – a to je zasláno zpět uživateli, který jej připojí k dokumentu.

Obrázek 2-13

Představa vzniku elektronického podpisu (vlevo) a časového razítka (vpravo)



[11] Poskytovatel časových razítek obvykle k zaslanému otisku nejprve připojí údaj o čase, z výsledku vytvoří nový otisk a teprve ten podepíše.

Povšimněme si ještě jednoho důležitého rozdílu mezi podpisy a razítky: elektronický podpis už z principu věci vždy vytváří podepisující osoba (neboli „ten, kdo se podepisuje“). Nejčastěji tedy ten, kdo dokument vytvořil, případně ten kdo ho schvaluje, vydává apod. Obecně ten, kdo s ním vyjadřuje svůj souhlas.

Naproti tomu časové razítko může k elektronickému dokumentu připojovat kdokoli za účelem „fixace v čase“ (stvrzení toho, že dokument v uvedené podobě existoval v daném čase). Nejedná se tedy o vyjádření souhlasu, a to ani ze strany aktuálního držitele dokumentu, který si nechává časové razítko vystavit (a může s obsahem dokumentu třeba i zásadně nesouhlasit), ani ze strany poskytovatele časových razítek.

Naopak po „věcné stránce“, je časové razítko vlastně shodné s elektronickým podpisem: vzniká principiálně stejným výpočtem, z principiálně stejných „ingrediencí“. Proto časové razítko zajišťuje například i integritu toho dokumentu, který je razítkem opatřen – a to i když to zákon explicitně neříká. Konstatuje to ale nepřímo, když zaručuje, že data opatřená časovým razítkem již existovala v okamžiku jeho vzniku, resp. před ním: kdyby došlo k jakékoli změně těchto dat (či samotného razítka), neboli k porušení jejich integrity, nebyla by to už „ta samá data“ (či „to samé razítko“).[12]

Z ryze praktického pohledu pak má vytváření časových razítek několik dalších zajímavých aspektů. Například ten, že probíhá v reálném čase a vyžaduje on-line přístup: ten, kdo chce nějaký svůj dokument opatřit časovým razítkem (kvalifikovaným časovým razítkem od kvalifikovaného poskytovatele), musí být schopen zaslat poskytovateli časových razítek příslušný otisk (hash). Poskytovatel na to musí reagovat v reálném čase (nikoli až třeba druhý den), vygenerovat časové razítko okamžitě a také ho co nejrychleji vrátit zpět žadateli.

Přitom jak uživatel, který o vytvoření časového razítka žádá, tak i poskytovatel časových razítek, musí být vzájemně propojeni takovým způsobem a přes taková rozhraní, aby si jejich systémy vzájemně rozuměly a dokázaly spolupracovat.

Naproti tomu při podepisování (vytváření elektronických podpisů) není nutné být on-line ani se propojit s dalšími subjekty, a není zde ani požadavek na fungování v reálném čase (už vzhledem k tomu, že údaj o čase vzniku podpisu není fakticky relevantní, kvůli tomu že není dostatečně důvěryhodný).

Stejně tak je zajímavý i aspekt ekonomický: za časová razítka se platí „průběžně“, obecně za každé jednotlivé časové razítko.[13] V případě elektronického podpisu zaplatí zákazník jen „jednorázově“ za vydání potřebného certifikátu, ale pak jej může využít (zdarma) k vytvoření tolika elektronických podpisů, kolik jich potřebuje.

---

12 V praxi to znamená, že i při vyhodnocování platnosti časového razítka se zjišťuje, zda je či není porušena integrita původního dokumentu.

13 Což samozřejmě nevylučuje různé paušální formy zpoplatnění.

> V praxi je tedy přidávání časových razítek na dokumenty podstatně náročnější než elektronické podepisování. I to nejspíše sehrálo svou roli při spouštění datových schránek, kdy autoři nastavili vše tak, aby orgány veřejné moci neměly za povinnost opatřovat produkované elektronické dokumenty kromě elektronických podpisů také časovými razítky. To následně zkomplikovalo využití takovýchto dokumentů v delším časovém horizontu.

2.8 Interní a externí elektronické podpisy

S elektronickými podpisy, ale i s elektronickými značkami a časovými razítky, úzce souvisí ještě jeden další aspekt, kterým jsme se dosud nezabývali. Jde v něm o to, jak vlastně připojit elektronický podpis (či elektronickou značku nebo razítko) k tomu dokumentu, který je tímto podpisem podepsán.

Připomeňme si, že při podepisování vzniká (výše popsaným způsobem) elektronický podpis, který můžeme chápat jako jedno velké číslo (viz kapitola 1). Ale také ho nemusíme chápat jako číslo, ale obecně jen jako „kus dat“ určité velikosti. V tuto chvíli nám to může být v zásadě jedno, protože právě teď řešíme jinou otázku: jak s tímto „kusem dat“ naložit? Jak zajistit, aby tento „kus dat“ byl chápán a interpretován jako elektronický podpis? Jak konkrétně realizovat to, co slovně snadno popíšeme jako „připojení elektronického podpisu k elektronickému dokumentu“?

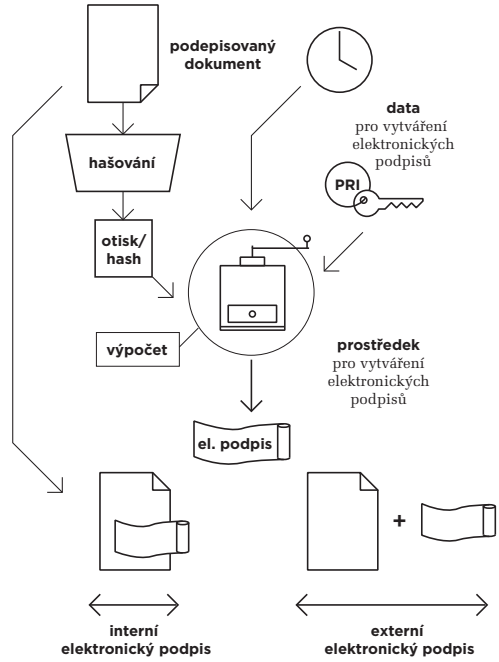
Odpověď je taková, že v úvahu připadají dvě principiální možnosti:

- **interní elektronický podpis:** tato varianta předpokládá, že „kus dat“, představující samotný elektronický podpis, je vložen přímo do dokumentu. Podmínkou k tomu samozřejmě je to, aby příslušný datový formát, ve kterém je dokument uložen, takovéto „vkládání“ umožňoval. Například formáty .DOC, .DOCX, .ODT a další, používané editory z nejrozšířenějších kancelářských balíků, tomu vychází vstříc. Stejně tak třeba formát PDF. Ale už třeba ne formát čistě textových dokumentů .TXT, který není nijak strukturovaný a nelze tedy do něj vkládat další druhy objektů.
- **externí elektronický podpis** (v angličtině **detached signature**): u této varianty je „kus dat“, představující samotný elektronický podpis, vložen do samostatného souboru. Tedy do jiného souboru, ve kterém je obsažen i jím podepsaný dokument. Výhodou je to, že formát dokumentu nemusí této variantě vycházet jakkoli vstříc.

Obě tyto varianty pochopitelně mají svá pro i svá proti (a analogicky to platí i pro elektronické značky a časová razítka). Tak třeba u interního podpisu se nám nemůže stát, že by se elektronický podpis někde „ztratil“ či zatoulal tak, že není k dispozici. Je-li uložen ve stejném souboru spolu se samotným dokumentem, je vždy k dispozici.

Na druhou stranu u interních podpisů může být problém s tím, když má být jeden dokument opatřen více podpisy současně. Pak jde opět o to, zda to příslušný formát podporuje (zda umožňuje vkládat více podpisů současně).

Obrázek 2-14
Představa interního a externího elektronického podpisu



Externí podpis zase má tu zřejmou výhodu, že nevyžaduje pro sebe jakoukoli podporu od použitého datového formátu. Pomocí externího podpisu tak může být podepsáno skutečně cokoli, co může mít podobu (nějakého, jakéhokoli) souboru. Jednoduché je také připojování více podpisů k témuž dokumentu, kde také nevznikají žádná principiální omezení.

Nevýhodou je naopak složitější udržování logické vazby mezi samotným podpisem a podepsaným dokumentem (či jiným objektem, obsaženým v souboru). Jak poznat, že „tento soubor“ obsahuje podpis „tamtoho souboru“? A jak to udělat, když takových podpisů je více? Nebo jde dokonce o časová razítka a je třeba ještě dodržet správné pořadí jejich aplikace?

Tomu se u externích elektronických podpisů pomáhá vhodným (stejným) pojmenováním: samotný soubor i jeho podpis a případné časové razítko (jako soubory) dostanou stejné jméno, a liší se jen svými příponami. Případně se vše řeší vhodným zapouzdřením: všechny soubory, které spolu logicky souvisí (tedy samotné dokumenty či jiné podepsané soubory, soubory s podpisy či značkami a soubory s časovými razítky), se „obalí“ nějakou společnou nadstavbou, která umožňuje zachytit jejich logickou vazbu (resp. vloží se do nějakého vhodného kontejneru).

> V běžné praxi se dnes využívá spíše interní elektronický podpis. A například datové schránky zpočátku ani nepočítaly s existencí externích podpisů.

3. Ověřování elektronických podpisů

Kapitola 3

3. Ověřování elektronických podpisů

Práce s elektronickými podpisy neobnáší pouze jejich vytváření a přidávání ke konkrétním elektronickým dokumentům, ať již na principu interního či externího elektronického podpisu. Stejně tak je nutné tyto podpisy následně vyhodnocovat. Tedy zabývat se tím, zda lze ověřit a prokázat jejich platnost – a následně se spoléhat na to, co je podepsáno a jednat podle toho.

Připomeňme si z předchozí kapitoly jednu velmi důležitou skutečnost, kterou se budeme podrobněji zabývat ještě v následující kapitole: že ověření platnosti a platnost elektronického podpisu jsou dvě relativně nezávislé věci. Elektronický podpis může být stále platný, i když už nejsme schopni ověřit a prokázat jeho platnost. Jinými slovy: naše neschopnost ověřit platnost podpisu nemusí být na závadu jeho platnosti. Ale na druhou stranu to může být na závadu tomu, abychom takovýto dokument mohli někomu předložit, a on jej musel od nás přijmout. Může totiž trvat na tom, abychom jeho platnost prokázali (což nedokážeme).[1] Celé to zkrátka je poněkud složitější.

Stejně tak si musíme uvědomit, že vyhodnocování platnosti (ověřování) elektronických podpisů je velmi „mezi-oborovou" záležitostí: má své technické aspekty, ale také významné aspekty právní. Těmi se budeme podrobněji zabývat v další kapitole (o právních aspektech elektronického podpisu). Zde se proto soustředíme jen na ony věcné (technické) aspekty ověřování elektronického podpisu.

3.1 Základní pravidla ověřování platnosti elektronických podpisů

Ze všeho nejdříve si naznačíme některé základní skutečnosti a pravidla, abychom získali vhodný nadhled a potřebné povědomí o celé problematice ověřování platnosti elektronických podpisů. Například bychom měli vědět, že celé vyhodnocování elektronického podpisu může skončit třemi různými variantami výsledku:

1. zjištěním, že elektronický podpis je **platný**: jsme schopni ověřit a prokázat platnost podpisu.
2. zjištěním, že elektronický podpis je **neplatný**: jsme schopni ověřit a prokázat neplatnost podpisu.
3. zjištěním, že **„nevíme"** (že platnost podpisu nedokážeme posoudit, že nejsme schopni ověřit, zda podpis je či není platný).

Stejně tak si musíme ujasnit, k jakému časovému okamžiku budeme platnost podpisu posuzovat (dále jen **posuzovaný okamžik**). V praxi ale nikdy nemáme jistotu o tom, kdy přesně podpis vznikl (viz předchozí diskuse o nespolehlivosti časového údaje uvnitř podpisu). Potřebnou jistotu můžeme získat pouze o tom, že podpis již existoval v nějakém pozdějším okamžiku, například skrze časový údaj na časovém razítku. Platnost podpisu pak posuzujeme k tomuto okamžiku. V opačném případě musíme posuzovat platnost certifikátu k aktuálnímu času.

---

[1] Protože jinak, podle ustanovení §5 zákona č. 227/2000 Sb., o elektronickém podpisu, by příjemce nesl případnou škodu způsobenou tím, že neprovedl všechny úkony potřebné k ověření platnosti podpisu.

Obrázek 3-1
Ikony, prostřednictvím kterých program Adobe Reader signalizuje výsledek ověření elektronického podpisu

Při samotném zkoumání platnosti elektronického podpisu musí být provedeno více různých úkonů, či alespoň vzato do úvahy více různých skutečností a faktorů:

- musí být ověřena integrita podepsaného dokumentu. Ta je pro platnost elektronického podpisu podmínkou nutnou, nikoli ale postačující:
  - je-li integrita porušena, můžeme rovnou konstatovat, že podpis je neplatný, ve smyslu varianty 2 předchozího výčtu (proto podmínka nutná).
  - opačně to ale rozhodně neplatí: je-li integrita podepsaného dokumentu neporušená, podpis může být platný, ale také nemusí. Stále tedy připadá v úvahu jak varianta 1, tak i varianty 2 a 3 (ve smyslu předchozího výčtu), a rozhodují mezi nimi další faktory.

- musí být ověřena platnost certifikátu, na kterém je podpis založen, a to k posuzovanému okamžiku. Jde opět o podmínku nutnou, ale ne postačující (pro variantu 1 v předchozím výčtu, tedy pro platnost podpisu).
  - nejprve je tedy nutné určit posuzovaný okamžik

- platnost certifikátu k posuzovanému okamžiku je třeba hodnotit ze dvou různých pohledů současně:
  - podle jeho řádné platnosti, která je v certifikátu uvedena, a dále
  - podle toho, zda k posuzovanému okamžiku nebyl certifikát revokován (předčasně zneplatněn)

- k tomu, aby mohl být certifikát shledán platným, musí být splněny obě dílčí podmínky: jeho řádná platnost (k posuzovanému okamžiku) ještě nesměla skončit, a certifikát nesměl být (k posuzovanému okamžiku) revokován.
  - pokud kterákoli z podmínek splněna není, certifikát nemůže být hodnocen jako platný.

- stejným způsobem musí být ověřena platnost všech nadřazených certifikátů na certifikační cestě (tj. nadřazených tomu certifikátu, na kterém je založen zkoumaný elektronický podpis)
  - není-li kterýkoli z nadřazených certifikátů (k posuzovanému okamžiku) platný, je výsledek ověření platnosti podpisu různý podle toho, co je důvodem neplatnosti certifikátu:
    - pokud byl některý z nadřazených certifikátů k posuzovanému okamžiku revokován (předčasně zneplatněn), pak je nutné konstatovat, že podpis je neplatný (ve smyslu varianty 2).
    - pokud k posuzovanému okamžiku již skončila řádná platnost nadřazeného certifikátu, musíme konstatovat, že „nevíme“ (nedokážeme ověřit platnost podpisu).

Konstatovat platnost elektronického podpisu (ve smyslu varianty 1, tedy ve smyslu naší schopnosti ověřit a prokázat platnost) můžeme pouze při „kladném“ souběhu tří logických podmínek:

- integrita podepsaného dokumentu nebyla porušena
- certifikát, na kterém je podpis založen, byl k posuzovanému okamžiku platný (ještě neuplynula doba jeho řádné platnosti). Aby mohl být platný, musí být platné i všechny jeho nadřazené certifikáty.
- certifikát, na kterém je podpis založen, nebyl k posuzovanému okamžiku revokován (předčasně zneplatněn). Totéž musí platit i pro všechny nadřazené certifikáty.

Po procedurální stránce je možné rozdělit posuzování těchto podmínek do několika různých kroků:

- posouzení integrity podepsaného dokumentu (zda byla, či nebyla porušena).
  - pokud porušena byla, můžeme skončit s konstatováním, že podpis je neplatný
- určení „posuzovaného okamžiku“: musíme určit časový okamžik, ke kterému budeme platnost posuzovat
  - tento krok musí předcházet všem dalším, protože ty na něm závisí.
- zjištění, zda k posuzovanému okamžiku nedošlo k revokaci (předčasnému zneplatnění) některého z certifikátů na certifikační cestě
  - pokud došlo, musíme skončit s konstatováním, že podpis je neplatný.
- zjištění, zda k posuzovanému okamžiku ještě neskončila řádná doba platnosti některého z certifikátů na certifikační cestě
  - pokud již skončila, musíme skončit s výsledkem „nevíme“
  - pokud ne, můžeme skončit s konstatováním, že podpis je platný.

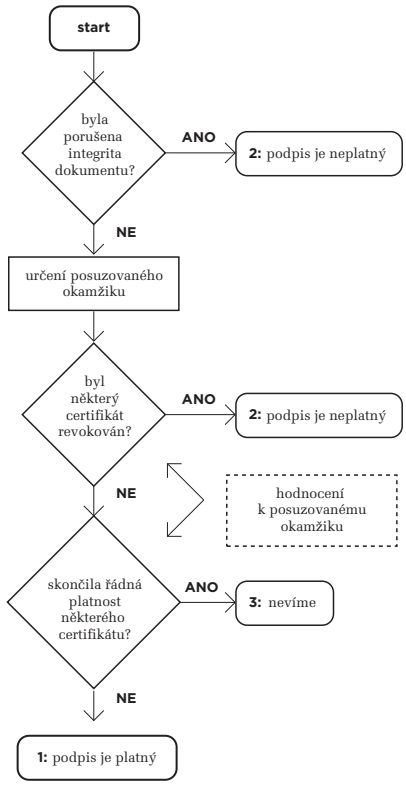
Celý postup naznačuje i vývojový diagram na následujícím obrázku.

Ještě v této kapitole si všechny tyto kroky rozebereme podrobněji. Již nyní si ale zdůrazněme jednu nesmírně důležitou skutečnost: že se stále bavíme o zaručeném elektronickém podpisu a že posouzení jeho platnosti je pouze „jednou stranou mince“. Zapomínat nesmíme ani na druhou stranu téže mince. Tou je statut elektronického podpisu, ze kterého vyplývá také jeho důvěryhodnost.

Při určitém zjednodušení si můžeme představit, že ověření platnosti (zaručeného) elektronického podpisu je technickou záležitostí, která zjišťuje pouze jeho „věcnou správnost“.

> Například u již několikrát zmiňovaného elektronického podpisu literární postavy Josefa Švejka bychom výše popsaným způsobem ověřování mohli (resp. měli) dospět ke zjištění, že tento (zaručený) elektronický podpis je platný. Ale těžko se můžeme spoléhat – v právním slova smyslu – na to, co je tímto podpisem opatřeno a jednat podle toho. Třeba s kupní smlouvou na nemovitost, podepsanou touto literární postavou, bychom na jakémkoli úřadě či třeba u soudu rozhodně nepochodili.

Obrázek 3-2
Vývojový diagram – postup ověřování platnosti elektronického podpisu



Abychom mohli posoudit „váhu“ (právní statut) elektronického podpisu, musíme ještě zjistit, zda jde jen o „obyčejný“ zaručený elektronický podpis, nebo o zaručený elektronický podpis, založený na kvalifikovaném certifikátu, či o uznávaný elektronický podpis (tj. zaručený elektronický podpis, založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb).

Právě vyhodnocovaný elektronický podpis tedy musíme ještě správně zařadit do celé škály elektronických podpisů s odstupňovanou mírou důvěryhodnosti. Tato důvěryhodnost pak vypovídá zejména o tom, jak moc se můžeme spoléhat na pravdivost údaje o podepsané osobě.

> Abychom uspěli na úřadě či u soudu, obecně u orgánu veřejné moci, potřebovali bychom dokument v elektronické podobě, opatřený uznávaným podpisem. Takový podpis (tj. uznávaný elektronický podpis) literární postavy Josefa Švejka již existovat nemůže.

Právním aspektům elektronických podpisů věnujeme celou následující kapitolu. Zde se naopak soustředíme na vyhodnocování (ověřování platnosti) zaručených elektronických podpisů ve výše popsaném smyslu. Jednotlivé fáze tohoto vyhodnocování, které jsme si výše naznačili jakoby „nahrubo“, si nyní upřesníme a detailněji rozvedeme.

3.2 Ověření integrity podepsaného dokumentu

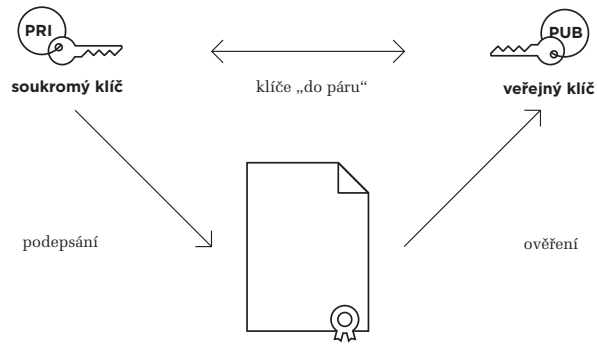
Relativně nejjednodušším úkonem (v rámci vyhodnocování platnosti elektronického podpisu) je ověření integrity podepsaného dokumentu. Tedy zjištění toho, zda od podpisu došlo k nějaké (jakékoli) změně dokumentu (což znamená porušení integrity), nebo zda k žádné změně nedošlo (což znamená neporušenou integritu).

Způsob ověření integrity přitom vychází ze základních principů asymetrické kryptografie, se kterými jsme se již seznámili v předchozí kapitole. Připomeňme si proto, skrze následující obrázek, vzájemně komplementární roli párových dat, neboli soukromého a veřejného klíče.

Tedy: při podepisování (vytváření elektronického podpisu) se použije soukromý klíč, jako jedna z výchozích „ingrediencí" (vedle otisku a údaje o čase). Je to možné díky tomu, že soukromý klíč je v držení toho, kdo podpis vytváří (podepisující osoby).

Při ověřování elektronického podpisu by se ale soukromý klíč již použít nedal, a to z jednoduchého, ale zcela principiálního důvodu: oprávněný držitel tohoto soukromého klíče jej „nesmí dát z ruky". Takže pokud chceme, aby možnost ověření měl skutečně kdokoli, musí být vše zařízeno tak, aby se k tomuto ověření dal použít klíč veřejný. Ten zase nejde použít pro podepisování, a tak může být skutečně rozdáván komukoli (být opravdu veřejný).

Obrázek 3-3
Představa využití soukromého a veřejného klíče

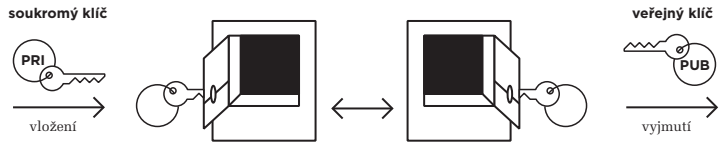


Tolik jednoduché vysvětlení (či spíše připomenutí) role obou klíčů. Ve skutečnosti je ale kolem tohoto jejich fungování velká a složitá „věda" (konkrétně z oblasti asymetrické kryptografie), a pouze ona dokáže spolehlivě vysvětlit a hlavně prokázat, že se oba klíče skutečně chovají popsaným způsobem.

Pro naše účely ale nemusíme zabíhat do složitých detailů asymetrické kryptografie, protože základní myšlenku si můžeme ukázat na zjednodušené představě bezpečnostní schránky se dvěma jednosměrnými dvířky: soukromý klíč otevírá jedna dvířka, a veřejný klíč ta druhá. Se samotnou schránkou se pak pracuje tak, že co se do ní dá z jedné strany vložit (skrze jedna dvířka a s využitím jednoho klíče), to se dá vyjmout jen z druhé strany (skrze druhá dvířka, pomocí druhého klíče).

Představu využití takovéto schránky pro podepisování ukazuje následující obrázek:

Obrázek 3-4
Představa podepisování



- **podepsání** odpovídá vložení dokumentu do schránky těmi (jednosměrnými) dvířky, kterými lze pouze vkládat a které otevírá soukromý klíč. Ten má k dispozici pouze podepisující osoba, a tedy pouze ona může dokument do schránky vložit.
- **ověření**, resp. **vyhodnocení platnosti** podpisu, odpovídá vyjmutí dokumentu ze schránky druhými (jednosměrnými) dvířky, kterými lze pouze vyjímat a které otevírá veřejný klíč. Ten může existovat v neomezeně mnoha exemplářích a může být libovolně distribuován, takže jej může využít skutečně kdokoli. A jelikož přitom ze schránky vyjímá dokument, který tam mohl vložit (skrze první dvířka) pouze ten, kdo vládne soukromým klíčem, může mít jistotu, že dokument do schránky vložil (podepsal) pouze tento držitel soukromého klíče.

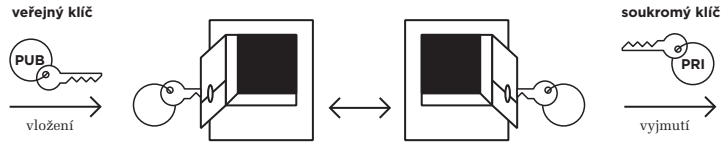
Když už jsme u této intuitivní představy s bezpečnostní schránkou, udělejme si malou odbočku a ukažme si dopředu to, čím se budeme podrobněji zabývat v kapitole 8: jak se dá asymetrická kryptografie využít k **šifrování**. Přitom si současně můžeme zdůraznit, že elektronický podpis žádné šifrování ani jinou formu zajištění tzv. **důvěrnosti** neprovádí.

Nicméně pomocí stejných párových dat (soukromého a veřejného klíče), jaké se používají pro podepisování, se dá realizovat i šifrování, pro potřeby zajištění důvěrnosti. Jen se oba klíče (a jimi otevíraná dvířka) musí použít jakoby v opačném gardu: ten, kdo chce něco zašifrovat, k tomu použije veřejný klíč příjemce. To v naší analogii s bezpečnostní schránkou odpovídá vložení dokumentu do schránky těmi dvířky, které otevírá veřejný klíč. Zašifrovat dokument (vložit jej do schránky) nyní může kdokoli, protože veřejný klíč je k dispozici každému.

Jakmile je ale konkrétní dokument již vložen do bezpečnostní schránky (je zašifrován), už ho dokáže ze schránky vyjmout (dešifrovat) druhými dvířky jen určený příjemce – protože k tomu je nutný odpovídající soukromý klíč, a ten má ve své moci pouze on.[2]

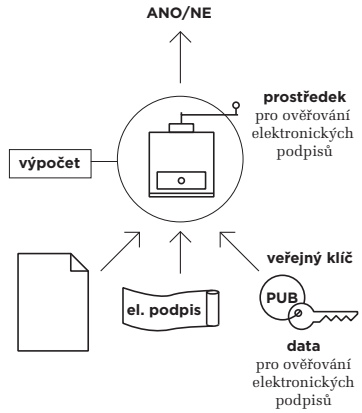
[2] Alternativní představou (ke zde použité analogii s bezpečnostní schránkou se dvěma dvířky) může být představa visacího zámku a klíče od něj: samotný visací zámek lze nasadit a zaklapnout (zamknout) i bez klíče, ale otevřít ho (odemknout) lze jen s klíčem. Zašifrování nějakého dokumentu pak odpovídá nasazení a zaklapnutí zámku, zatímco dešifrování odpovídá odemknutí zámku klíčem. Ten, kdo chce, aby mu protistrana něco zašifrovala, jí pošle svůj zámek (jako analogii veřejného klíče). Protistrana zámek nasadí a zaklapne. Otevřít ho pak dokáže již jen oprávněný příjemce, který má od zámku klíč (odpovídající soukromému klíči).

Obrázek 3-5
Představa šifrování

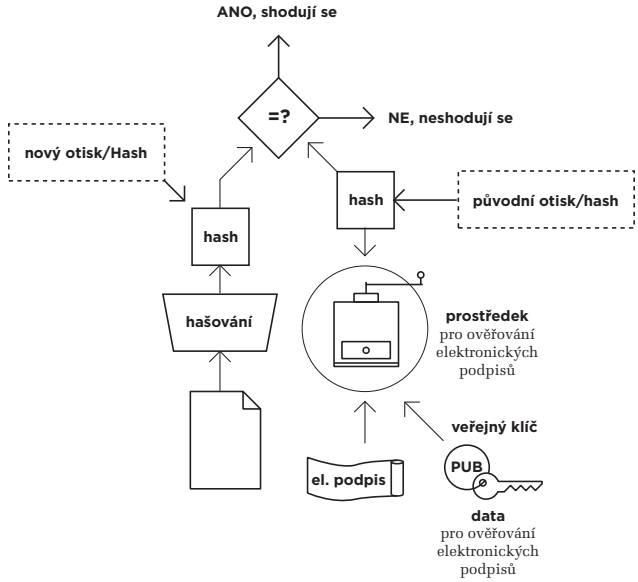


Vraťme se ale od šifrování zpět k elektronickým podpisům a řekněme si, jak doopravdy probíhá ono „vyjímání z bezpečnostní schránky“ s využitím veřejného klíče. Základní představu ukazuje obrázek.

Obrázek 3-6
Rámcová představa vyhodnocování integrity podepsaného dokumentu



Obrázek 3-7
Detailnější představa ověřování integrity podepsaného dokumentu



Vstupem jsou zde tři „ingredience“, a to samotný dokument, dále jeho elektronický podpis, a pak příslušný veřejný klíč. To, co se s nimi provádí, si opět můžeme představit jako určité „semletí“, i když ve skutečnosti jde o poměrně složitý výpočet.

Jeho výsledkem ale není nějaké číslo, nýbrž pouze výrok: ANO či NE. Pokud bychom se totiž na celý postup vyhodnocování integrity podívali detailněji, zjistili bychom, že v rámci celého postupu je nejprve „semlet“ samotný elektronický podpis s veřejným klíčem. Výsledkem je otisk (hash), vypočítaný z původního dokumentu ještě při jeho podepisování.[3] No a tento „původní“ otisk pak můžeme srovnat s „novým“ otiskem, který (nově) vytvoříme ze samotného dokumentu. Výsledný výrok ANO či NE pak říká, zda se oba otisky shodují, či neshodují.

Jak ale toto ANO (či naopak NE) správně interpretovat? K čemu se vztahuje? Zdůrazněme si, že ještě zdaleka nejde o výrok ohledně toho, zda je elektronický podpis na dokumentu platný, či nikoli. To opravdu ne.

Zde jde pouze o vyjádření ohledně integrity podepsaného dokumentu:

- ANO znamená, že integrita podepsaného dokumentu nebyla porušena (zůstala zachována), a dokument se tedy od svého podpisu nezměnil
- NE znamená, že integrita dokumentu byla porušena, a dokument se tedy od svého podpisu nějak změnil. Vlastně tedy už jde o nějaký jiný dokument.

Připomeňme si, že zachování integrity podepsaného dokumentu je pro celkovou platnost elektronického podpisu podmínkou nutnou, ale nikoli postačující. Takže pokud v této fázi uslyšíme NE, můžeme se zkoumáním platnosti podpisu rovnou skončit a konstatovat, že je neplatný.

Pokud ale v této fázi uslyšíme ANO, ještě nemáme zdaleka vyhráno a ve zkoumání platnosti podpisu musíme pokračovat dále, ověřením dalších nutných podmínek pro platnost. Které to jsou, jsme si již naznačili výše: certifikát, na kterém je podpis založen, musí být platný a nesměl být revokován (předčasně zneplatněn). Stejně tak všechny nadřazené certifikáty.

3.3 Posuzovaný okamžik

Aby to ale nebylo až tak jednoduché, při zkoumání případné revokace a řádné platnosti certifikátu musíme ještě zohlednit časový faktor.

---

[3] Zde opět můžeme využít naši analogii s vkládáním do schránky se dvěma (jednosměrnými) dvířky: původní otisk jsme (s využitím soukromého klíče) vložili do schránky jedněmi dvířky, zatímco druhými dvířky (s využitím veřejného klíče) ho zase vyndáme – v jeho původní podobě.

Z podstaty věci bychom vždy měli posuzovat platnost podpisu k okamžiku jeho vzniku. Jenže to není možné. Jak jsme si již uvedli, na časový údaj, obsažený přímo v samotném elektronickém podpisu, se spoléhat nemůžeme – mohl být nastaven libovolně.

Pak nám nezbývá, než zkoumat platnost podpisu k nějakému pozdějšímu okamžiku (posuzovanému okamžiku, viz výše). Takovému, že pro něj už máme jistotu, že podpis existoval. Obvykle díky časovému razítku, které bylo aplikováno „přes" elektronický podpis (neboli po něm, ve smyslu časové souslednosti, a navíc tak, aby mohlo být detekováno porušení integrity jak samotného dokumentu, tak i jeho elektronického podpisu). Pak se spoléháme na to, že když je podpis shledán platným k tomuto pozdějšímu (posuzovanému) okamžiku, musel být platným i v okamžiku svého vzniku (byť tento okamžik spolehlivě neznáme).[4]

Daní za toto „pozdější" ověření je ale nebezpečí, vyplývající z plynutí času: v době svého vzniku podpis platný byl, ale k pozdějšímu okamžiku, ke kterému jeho platnost zkoumáme, už nemusíme být schopni to ověřit a prokázat. Třeba proto, že příslušnému certifikátu v mezidobí již skončila jeho řádná platnost.

V tomto případě (tedy pokud k posuzovanému okamžiku již skončila řádná platnost certifikátu), musíme férově konstatovat, že „nevíme", resp. nejsme schopni ověřit platnost podpisu (ve smyslu varianty 3 možných výsledků). Připomeňme si ale, že tato naše neschopnost nás neopravňuje ke konstatování, že zkoumaný podpis je neplatný.

V praxi pak bývá dosti častá i ta varianta, kdy nemáme vůbec žádné (spolehlivé) vodítko ohledně toho, kdy podpis vlastně vznikl. Tedy ani žádné časové razítko, které by „překrývalo" podpis. Pak nám nezbývá než vyhodnocovat platnost podpisu k aktuálnímu okamžiku (k okamžiku vyhodnocování). A zde je nebezpečí „uplynutí času" mnohem větší.

Vlastně se toto nebezpečí rychle mění v jistotu: jelikož v ČR jsou certifikáty, používané pro elektronické podpisy, obvykle vydávány s platností na 1 rok, pak nejdéle do tohoto 1 roku od vzniku podpisu ztrácíme možnost ověřit platnost takového podpisu, který není „překryt" časovým razítkem.[5] V praxi to ale může být i mnohem dříve, protože záleží na tom, jak „čerstvý" byl certifikát v době vzniku podpisu. Pokud do konce jeho platnosti zbývalo třeba jen 5 dnů, a podpis nebyl „překryt" časovým razítkem, pak po 5 dnech již není možné platnost podpisu ověřit.

Nepříjemný je tento „odložený" způsob posuzovaní platnosti v případě, kdy došlo k revokaci certifikátu: pokud zjistíme, že k posuzovanému okamžiku byl certifikát již revokovaný, musíme naopak skončit konstatováním, že elektronický podpis je neplatný (ve smyslu varianty 2). Nedokážeme totiž posoudit, zda podpis vznikl ještě před revokací, nebo až po ní.

---

[4] Zde si připomeňme, že podpis a časové razítko nevznikají současně, ale vždy je mezi nimi určitý časový odstup. A my nevíme, zda jde o zlomky sekund, či třeba celé hodiny, dny, roky atd.

[5] Absence časového razítka je bohužel typická pro dokumenty, produkované orgány veřejné moci a přenášené skrze datové schránky.

Ukažme si vše na příkladech:

> Představme si elektronicky podepsaný dokument, opatřený platným časovým razítkem, které bylo vystaveno k 1. 7. 2010. V rámci ověřování platnosti podpisu ale zjistíme, že příslušný certifikát, na kterém je podpis na dokumentu založen, byl revokován k 1. 6. 2010, 12:00. Pak musíme podpis prohlásit na neplatný, protože nedokážeme rozhodnout, zda vznikl již před datem 1. 6. 2010 12:00, nebo až po něm.
>
> Nebo jiný příklad: časové razítko zní na 1. 7. 2010, zatímco certifikát byl revokován k 1. 8. 2010. Tento souběh již nebrání ověření platnosti podpisu, protože spolehlivě víme, že podpis vznikl ještě před revokací certifikátu. K platnosti podpisu je ale nutná ještě neporušená integrita.

U těchto dvou příkladů nezáleželo na tom, kdy k vyhodnocení dochází, protože „posuzovaným okamžikem" byl okamžik, uvedený na časovém razítku. Díky jeho existenci jsme měli jistotu, že podpis na dokumentu vznikl "někdy před" okamžikem, uvedeným na časovém razítku.

Ukažme si ale také příklad toho, kdy podepsaný dokument není opatřen časovým razítkem, a za posuzovaný okamžik proto musí být zvolen aktuální časový okamžik.

> Představme si elektronicky podepsaný dokument. Jeho podpis je založen na certifikátu, který byl vydán podepisující osobě 1. 8. 2009 na dobu 1 roku (tj. do 1. 8. 2010). Dokument ale není opatřen časovým razítkem. Předpokládejme také, že certifikát nebyl v době své řádné platnosti revokován.
>
> Pokud byla platnost tohoto podpisu ověřována například dne 1. 7. 2010, pak muselo být zjištěno, že nedošlo k revokaci certifikátu. Stejně tak bylo zjištěno, že řádná platnost certifikátu ještě neskončila. Z toho plyne, že certifikát musel být platný (a nerevokovaný) i v době vzniku podpisu. Pokud byly splněny všechny další podmínky (tj. neporušená integrita), mohl být podpis ověřen jako platný.
>
> Pokud byla platnost podpisu ověřována například dne 1. 9. 2010 (či kdykoli později), pak muselo být zjištěno, že řádná platnost certifikátu již skončila. Výsledkem posouzení platnosti pak musí být varianta 3 („nevíme", resp. platnost k aktuálnímu okamžiku není možné ověřit).

Teď si vše ještě zkomplikujme variantou, kdy certifikát byl revokován:

> Dokument je elektronicky podepsán. Podpis je založen na certifikátu, který byl vydán podepisující osobě 1. 8. 2009 na dobu 1 roku (tj. do 1. 8. 2010). Tento certifikát byl ale revokován, a to k 1. 5. 2010 12:00. Dokument není opatřen časovým razítkem.
>
> Pokud byla platnost tohoto podpisu ověřována například 1. 4. 2010, neboli v době ještě před revokací certifikátu, pak muselo být zjištěno, že certifikát nebyl revokován. Stejně tak muselo být zjištěno, že řádná platnost certifikátu ještě neskončila. Pokud byly splněny všechny další podmínky (neporušená integrita), měl být podpis ověřen jako platný.

> Pokud byla platnost tohoto podpisu ověřována 1. 6. 2010 (či později), pak muselo být zjištěno, že certifikát již byl revokován (k datu 1. 5. 2010, 12:00). Výsledkem posouzení platnosti proto musela být varianta 2: podpis je neplatný.

3.4 Ověření platnosti certifikátu

Připomeňme si, že každý certifikát má předem stanovenou dobu své platnosti. Ta je v něm „napevno zabudována“: v každém certifikátu je napsáno, že platí od určitého konkrétního data do jiného konkrétního data, a tyto údaje není možné jakkoli měnit.

> U certifikátů, vydávaných tuzemskými certifikačními autoritami a využívaných pro elektronické podpisy či značky, je délka jejich platnosti nastavována na 1 rok.[6] U certifikátů, využívaných pro časová razítka, to jsou zpravidla 3 roky (v případě CA PostSignum), nebo 5 let (v případě I. CA), či dokonce 6 let (v případě CA eIdentity).

Ověření, zda tato „řádná“ platnost certifikátu k posuzovanému okamžiku již skončila, nebo ještě ne, je jednoduchou záležitostí, která v praxi nečiní žádné problémy.

Na co ale nesmíme zapomínat (a co v praxi činí problémy) je možnost předčasného ukončení „řádné“ platnosti, a to skrze mechanismus revokace certifikátu (alias zneplatnění certifikátu, resp. jeho odvolání). Vždy se musíme přesvědčit, zda k posuzovanému okamžiku došlo či nedošlo k revokaci toho certifikátu, který zkoumáme. A je přitom jedno, zda stav revokace zkoumáme jako samostatnou podmínku (vedle „řádné platnosti“ certifikátu), nebo zda ji zahrneme pod jedinou podmínku (časové platnosti certifikátu).

> V úvodu této kapitoly jsme revokaci zkoumali jako samostatnou podmínku, nezávisle na řádné platnosti certifikátu. Důvodem je jak kompatibilita s tím, jak je ověřování platnosti popsáno v prováděcích vyhláškách,[7] tak především logika věci: jak již víme, výsledný verdikt o platnosti elektronického podpisu se liší podle toho, zda platnost certifikátu (přesněji: kteréhokoli z certifikátů na certifikační cestě) skončila uplynutím doby jeho řádné platnosti nebo jeho revokací (předčasným zneplatněním).

---

[6] Jde o volbu příslušné certifikační autority, která musí zohlednit riziko zneužití certifikátu, které s časem roste (podrobněji viz část 2.6). Některé zahraniční certifikační autority hodnotí rizika jinak a vydávají podpisové certifikáty i s platností na 2 roky, či dokonce 3 roky.

[7] Konkrétně ve vyhlášce č. 496/2004 Sb., “o elektronických podatelnách“.

3.4.1 Možnost revokace certifikátu

Možnost revokace (předčasného zneplatnění, odvolání) konkrétního certifikátu je pojistkou proti případným nestandardním situacím, ale také řešením pro některé vcelku standardní situace.

Například: pokud dojde ke kompromitaci soukromého klíče (například když jej někdo ukradne nebo si jej „jen“ zkopíruje), jeho oprávněný vlastník už nad ním nemá výlučnou kontrolu. A to je vážný problém, protože nový držitel soukromého klíče by se mohl platně podepisovat jeho jménem. Jedinou cestou, jak tomu zabránit, je předčasně ukončit platnost příslušného certifikátu, který je s tímto soukromým klíčem spojen, cestou jeho revokace. Můžeme si to představit i jako oznámení, adresované komukoli, kdo by chtěl s certifikátem dále pracovat (a ověřovat podle něj nějaký konkrétní podpis): **od okamžiku, kdy k revokaci došlo, už nevěřte tomu, co je na certifikátu napsáno.** A také: **od tohoto okamžiku už nenesu odpovědnost za to, co je podepsáno s využitím mého soukromého klíče.**

Motivace pro revokaci ale nemusí být až takto vyloženě negativní. Třeba když nějaký úředník používá v rámci své působnosti konkrétní certifikát, ale pak odejde na jiné pracoviště, do důchodu či jakkoli jinak přestane plnit úkoly, pro které mu byl certifikát vystaven, je vhodným opatřením požádat o revokaci příslušného certifikátu. I jako prevenci proti jeho případnému zneužití.

Důvodem pro revokaci certifikátu někdy bývá i přechod na používání novějšího certifikátu. Jak jsme si již uvedli, certifikát sice lze využívat při podepisování až do konce jeho řádné platnosti, ale není to rozhodně ideální: pokud není podepsaný dokument opatřen časovým razítkem, které by fixovalo podpis v čase, se skončením řádné doby platnosti certifikátu (tedy třeba již za několik dnů či pouze hodin od podpisu) ztrácíme možnost ověřit platnost podpisu, který je na takovémto certifikátu založen. Proto je více než vhodné přestat používat konkrétní certifikát podstatně dříve, než skončí řádná doba jeho platnosti. Následně je možné nechat již nepoužívaný certifikát revokovat.[8]

S technickou realizací revokace je ale spojen nepříjemný problém: jak zajistit, aby se informace o předčasném ukončení platnosti certifikátu (o jeho revokaci) dostala včas (resp. okamžitě) do všech exemplářů příslušného certifikátu, které kde mohou existovat? Zde si zopakujme, že certifikáty jsou z principu veřejné a volně šiřitelné. Takže kdokoli si je může kopírovat, kam jen chce a v jakém počtu jen chce. Za těchto okolností je ale zhola nemožné je následně všechny dohledat.

Navíc, i kdyby se přeci jen podařilo dohledat všechny exempláře již odvolaného certifikátu, stejně by to bylo k ničemu: každý certifikát je „pouze pro čtení“ a nejde v něm dělat změny. Již jen proto, že jako celek je podepsán (opatřen elektronickou značkou certifikační autority, která ho vydala), a jakákoli změna certifikátu by znamenala porušení jeho integrity a okamžité zneplatnění jeho podpisu.

---

[8] Pokud je ale již nepoužívaný certifikát skutečně revokován, může to přinést velký problém: všechny do té doby vytvořené podpisy, které nejsou včas opatřeny časovým razítkem, musí být vyhodnoceny jako neplatné, protože již není možné spolehlivě zjistit, zda byl podpis vytvořen ještě před revokací, či až po ní.

Možnost revokace jakéhokoli certifikátu proto musí být implementována na úplně jiném principu, než je nějaké dohledávání všech exemplářů a jejich dodatečné měnění.

Konkrétní řešení je takové, že informace o revokaci (tj. zda certifikát byl či nebyl revokovaný, a k jakému datu) zůstává u jeho vydavatele, tj. u příslušné certifikační autority, na předem určeném místě. Každý, kdo s nějakým certifikátem pracuje, pak má povinnost podívat se na toto předem určené místo a zde si ověřit, zda certifikát nebyl revokován.

Umístění informace o případné revokaci (u vydavatele certifikátu) reflektuje i skutečnost, že pouze původní vydavatel (certifikační autorita) je schopen korektně vést nezbytnou agendu, která je s revokací spojena. Tedy například zajistit to, aby o revokaci mohl požádat právě a pouze ten, kdo je k tomu oprávněn.

I při revokaci je totiž nutné pečlivě a spolehlivě ověřit identitu toho, kdo o revokaci žádá – a k tomu má dostatek podkladů právě a pouze původní vydavatel certifikátu. Právě on je také ve smluvním vztahu s tím, kdo si certifikát nechal vystavit, a pouze v rámci tohoto smluvního vztahu tak mohou být ošetřeny všechny potřebné náležitosti pro revokaci. Včetně toho, jak musí být žádost o revokaci podána, a jak ji certifikační autorita (vydavatel certifikátu) zpracovává, v jakých lhůtách atd.

3.4.2 Protokol OCSP a seznamy CRL

V každém certifikátu je vždy uvedena přesná adresa místa, kam je třeba se podívat, zda certifikát nebyl revokován. Toto „podívání se“ ale může mít dvě principiálně odlišné formy:

- fungující v reálném čase
- fungující „opožděně“

Rozdíl mezi oběma variantami je zásadní: v prvním případě máme možnost se okamžitě dozvědět, zda k okamžiku, kdy dotaz klademe, byl certifikát revokován, či nebyl. Ve druhém případě máme možnost se požadovanou informaci dozvědět pouze zpětně, s určitým časovým odstupem.

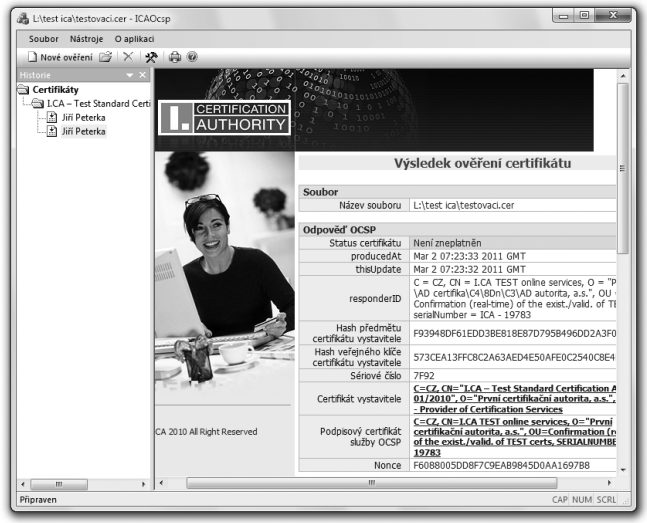
Pro realizaci první varianty samozřejmě musí existovat potřebná technická řešení. Nejčastěji je používán protokol **OCSP (Online Certificate Status Protocol)**, který umožňuje vznést interaktivní dotaz na certifikační autoritu a ihned získat požadovanou odpověď.[9] V ČR se s implementací tohoto protokolu teprve začíná,[10] počátkem roku 2011 jej zkoušela v testovacím provozu první tuzemská certifikační autorita (I. CA).

---

9 Obvykle ale jen tomu, kdo má s příslušnou certifikační autoritou uzavřenu smlouvu na poskytování služeb na bázi OCSP protokolu, protože jde typicky o zpoplatněnou službu.

10 Nejspíše je tomu tak proto, že tato první varianta není požadována zákonem. Ten požaduje pouze druhou variantu.

Obrázek 3-8
Příklad výsledku ověření stavu revokace prostřednictvím protokolu OCSP u I.CA



Standardně využívaná je až druhá varianta (fungující „opožděně“), jejíž dostupnost je přímo vyžadována zákonem. Z hlediska implementace je jednodušší, alespoň pro samotné certifikační autority. Uživatelům, kteří se chtějí spoléhat na platnost elektronických podpisů, ale přináší dosti zásadní komplikaci: pokud budou ověřovat platnost nějakého konkrétního elektronického podpisu, nemají šanci to zvládnout v reálném čase (tj. dozvědět se výsledek ihned). Musí nejprve počkat, a to relativně dlouhou dobu: až 24 hodin.

Tato druhá varianta je v praxi implementována skrze tzv. **CRL seznamy**, kde CRL je zkratkou z anglického **Certificate Revocation List**. V doslovném překladu tedy jde o **seznam revokovaných certifikátů.**

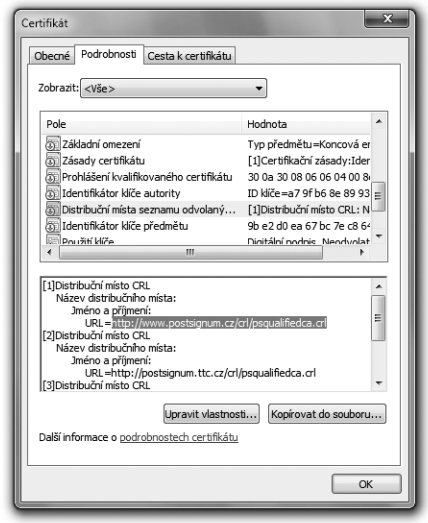
Již toto pojmenování přitom vystihuje věcnou podstatu: certifikační autorita jednoduše vyvěsí na konkrétní (předem dané) místo na svém webu seznam těch certifikátů, které byly revokovány – s uvedením přesné doby, ke které k revokaci došlo, a mnohdy také s uvedením důvodu revokace (byť toto není povinné). A do každého certifikátu již při jeho vydávání vloží odkaz na toto předem dané místo, formou URL odkazu, viz obrázek na následující stránce.

Problém je ale v tom, že takovéto „vyvěšení“ (zveřejnění informací formou CRL seznamu) nemusí být okamžité, ve vztahu k okamžiku, ke kterému k revokaci došlo. Přesněji: okamžitá nemusí být aktualizace tohoto seznamu, resp. vydání jeho nové verze.

V případě kompromitace nějakého soukromého klíče certifikační autority sice mohou vydat (a zveřejnit) novou verzi svého CRL seznamu velmi brzy, třeba i v řádu minut – ale nejsou povinny tak učinit okamžitě. Podle platných norem[11] mají na zpracování požadavku na revokaci právě oněch 24 hodin.

[11] CEN CWA 14167-1, kap. 5.2.5.2 – RM 1.1

Obrázek 3-9
Příklad URL odkazu na místo, kde je zveřejněn seznam revokovaných certifikátů (CRL seznam)



3.4.3 Postup při ověřování revokace certifikátu

Zjišťovat, zda konkrétní certifikát byl či nebyl revokován, bychom správně měli k okamžiku, kdy vznikl elektronický podpis, jehož platnost zkoumáme. Jenže, jak už jsme si uvedli, tento okamžik přesně (a dostatečně spolehlivě) neznáme. Proto vždy posuzujeme platnost podpisu k nějakému pozdějšímu „posuzovanému okamžiku“ (pokud jej máme k dispozici), nebo k aktuálnímu časovému okamžiku.

Pokud zkoumáme platnost podpisu k takovému posuzovanému okamžiku, od kterého uplynulo více jak 24 hodin, pak nám nevadí to, že tuzemské certifikační autority dosud běžně neposkytují revokační informace v reálném čase (skrze protokol OCSP), ale jen ve formě CRL seznamů, které vydávají s tak velkými časovými odstupy. Stačí nám podívat se na první CRL seznam, vydaný po uplynutí oněch 24 hodin. Pokud na takovémto CRL seznamu nenajdeme informaci o tom, že zkoumaný certifikát byl revokován, pak můžeme ihned konstatovat splnění dílčí podmínky (že certifikát nebyl revokován).

Jinak je tomu ale v případě, kdy nemáme žádné spolehlivé vodítko ohledně dřívější doby vzniku zkoumaného podpisu, jako například u elektronicky podepsaného dokumentu bez časového razítka. Pak musíme platnost podpisu vyhodnocovat k aktuálnímu okamžiku – ale pak se nemůžeme dívat do žádné starší (a díky tomu již zveřejněné) verze CRL seznamu.

Místo toho musíme počkat oněch 24 hodin na vydání nových CRL seznamů, resp. na jejich aktualizaci, zda se v nich teprve neobjeví ten certifikát, který nás zajímá.[12]

[12] Takovéto čekání je ale pro praxi velký problém. Například při autorizované konverzi takových elektronických dokumentů, které nejsou opatřeny časovým razítkem, by na CzechPointech bylo vždy třeba nejprve počkat 24 hodin, než může být požadovaná konverze provedena. Ta totiž vyžaduje ověření, zda je na konvertovaném dokumentu platný podpis.

3.4.4 Kumulativní a intervalové CRL seznamy

S potřebou „podívat se“ do starší verze CRL seznamu souvisí i otázka toho, jak jsou tyto seznamy vlastně vedeny, a také jak dlouho jsou k dispozici.

Pro vedení CRL seznamů existují dvě základní možnosti:

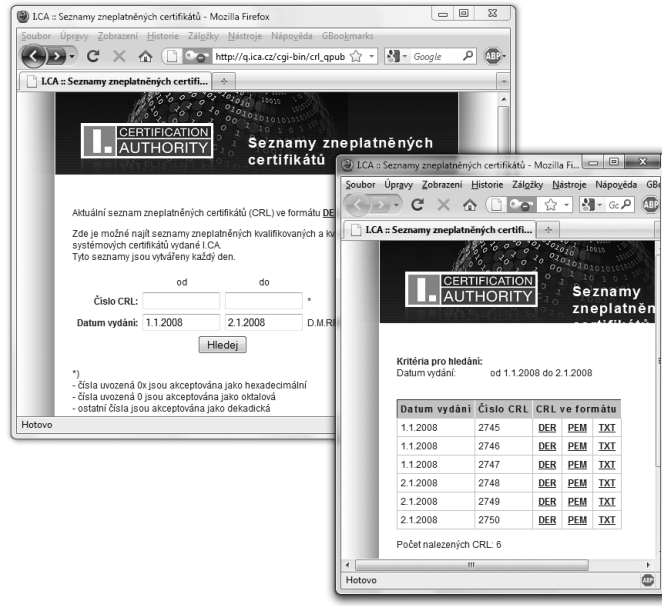
- „kumulativní seznam“: takovýto CRL seznam je jen jeden, je průběžně aktualizovaný a obsahuje celou historii revokovaných certifikátů (tj. jde o seznam revokovaných certifikátů sahající až do doby, kdy certifikační autorita začala certifikáty vydávat, resp. od kdy je povinna je zveřejňovat).
- „intervalové seznamy“: takovýchto CRL seznamů existuje více, a „pokrývají“ vždy jen určitý časový interval, typicky v délce platnosti příslušného druhu certifikátu. V aktuální verzi takovéhoto CRL seznamu tedy lze najít informace o (eventuální) revokaci jen takových certifikátů, které by jinak byly stále ještě platné. Pro informace o starších certifikátech je třeba najít příslušný starší (intervalový) seznam CRL.

Certifikační autority, akreditované v ČR, používají obě právě popsané varianty:

- společnost eIdentity vydává (jeden) kumulativní seznam CRL, který průběžně aktualizuje
- společnosti PostSignum a I.CA vydávají intervalový seznam CRL. Od něj je vždy dostupná aktuální verze (přes jedno URL), zatímco starší verze je třeba vyhledávat přes vyhledávací rozhraní na webu certifikační autority. Příklad ukazují obrázky.

Obrázek 3-10

Hledání starších CRL seznamů od I. CA



Kromě zveřejňování informací o revokaci konkrétních certifikátů ve formátu CRL seznamů umožňují některé certifikační autority získání těchto informací i interaktivně, skrze formulář na svých webových stránkách. Příkladem může být společnost eIdentity, viz obrázek.

Obrázek 3-11
Příklad informace o revokaci certifikátu, získané přes web

Pokud jde o „hloubku v čase“, po kterou vydavatelé certifikátů (certifikační autority) zveřejňují informace o revokování svých certifikátů, pak tuto otázku relevantní zákon (č. 227/2000 Sb. o elektronickém podpisu) explicitně neřeší.

Obecně ale říká, že certifikační autority jsou povinné uchovávat informace o svých službách po dobu 10 let, a po uplynutí této doby je bez zbytečného odkladu předávají ministerstvu vnitra.[13]

3.4.5 Jak dlouho je možné revokovat?

S vyhodnocováním platnosti elektronických podpisů a s možností revokace certifikátů souvisí ještě jedna velmi zajímavá otázka: mělo by být možné revokovat certifikát jen po dobu jeho řádné platnosti, nebo by tato možnost měla připadat v úvahu kdykoli, tedy i po skončení řádné doby platnosti certifikátu?

Pro první variantu (možnost revokace jen během řádné platnosti) hovoří jednoduchá logická úvaha: revokace je vlastně předčasné zneplatnění, takže by mělo být možné jen do té doby, dokud platnost neskončí řádným uplynutím původně nastavené doby platnosti. Jakmile tato doba skončí, certifikát se stává neplatným tak jako tak, a není tedy nutné jej nějak zneplatňovat „ještě více“.

Pravdou také je, že praxe všech tuzemských certifikačních autorit odpovídá této variantě: jejich mechanismy revokace (a to jak po technické stránce, tak i po stránce právní) jsou nastaveny tak, že zákazníci mohou požádat o revokaci svých certifikátů jen po dobu jejich řádné platnosti, a nikoli již po jejím skončení.

Jenže existuje i významný argument pro druhou variantu (možnost revokace i po skončení řádné platnosti): to, jakým způsobem skončí platnost certifikátu, má zásadní vliv na výsledek vyhodnocení platnosti podpisu, který je na tomto certifikátu založen (a u kterého není jasné, zda vznikl před koncem

[13] V době vzniku tohoto textu nebylo jasné, jak bude toto ustanovení zákona v praxi interpretováno: zda certifikační autority přestanou zveřejňovat informace o revokaci starší 10 let, či zda je pouze předají ministerstvu, ale budou je nadále samy zveřejňovat.

platnosti či po něm). Rozebírali jsme si to na začátku této kapitoly, a tak si jen stručně připomeňme na příkladu elektronicky podepsaného dokumentu, který není opatřen časovým razítkem:

- pokud platnost certifikátu skončila kvůli revokaci, pak ověřování podpisu končíme s verdiktem, že podpis je neplatný (varianta 2 z části 3.1).
- pokud platnost certifikátu skončila řádným uplynutím doby platnosti, pak při ověřování podpisu končíme s výsledkem „nevíme“ (varianta 3).

Teď si ale představme situaci někoho, komu ukradnou (či jen zkopírují) jeho soukromý klíč – ovšem již v době, kdy příslušnému certifikátu již skončila jeho řádná platnost.

Pokud by v této situaci platila druhá varianta a certifikát by bylo možné revokovat i po uplynutí jeho řádné platnosti, bylo by to bezpečnější: oprávněný držitel soukromého klíče by při scénáři z předchozího odstavce nechal svůj certifikát revokovat – a následně by každý pokus o vyhodnocení platnosti podvodného podpisu skončil s verdiktem, že podpis je neplatný (varianta 2 z části 3.1).

V případě první varianty je tomu ale jinak: oprávněný držitel nemůže svůj certifikát revokovat, a vyhodnocení podvodného podpisu tak skončí verdiktem „nevím“ (varianta 3), kvůli uplynutí řádné doby platnosti. Ovšem verdikt „nevím“ působí přeci jen jinak, než verdikt „podpis je neplatný“. Ve spojení s principem, že elektronický podpis neztrácí svou platnost tím, že my ztratíme schopnost tuto platnost pozitivně ověřit, se pak z verdiktu „nevím“ stává velmi nebezpečná kombinace: svádí ke spoléhání se na platnost podpisu (k jednání, jako kdyby platnost podpisu byla ověřena). To je ale velká chyba. Ve skutečnosti bychom i při verdiktu „nevím“ měli jednat tak, jako kdyby verdikt zněl: „podpis je neplatný“.

> Příkladem může být chybné stanovisko Odboru legislativy a koordinace předpisů MV ČR, které ještě v květnu 2010 zastávalo názor, že je možné autorizovaně konvertovat z elektronické do listinné podoby i takové dokumenty, které nejsou opatřeny časovým razítkem, a u kterých již skončila platnost certifikátu, na kterém je jejich podpis založen.[14] To by ale znamenalo, že by se daly řádně konvertovat (a tím fakticky legalizovat) i podvodně podepsané dokumenty z výše popsaného scénáře (tj. podepsané ukradeným soukromým klíčem v době, kdy se certifikát již nedá revokovat).

3.5 Platnost nadřazených certifikátů

Připomeňme si, že prakticky všechny kroky při ověřování platnosti konkrétního elektronického podpisu využívají něco z obsahu certifikátu, na kterém je podpis založen – ať již je to veřejný klíč, či údaje o řádné platnosti certifikátu, o dostupnosti informací o případné revokaci certifikátu atd. Proto je nezbytně nutné, abychom se při ověřování mohli na tyto údaje spolehnout.

---

[14] Toto stanovisko se objevilo v dokumentu „Datové schránky a činnost správních orgánů“ ve verzi z 13.5.2010. V další verzi téhož dokumentu, z 28. 6. 2010, se tento názor již neobjevuje a místo něj je konstatováno, že se „dosud nepodařilo nalézt optimální vztah mezi právním názorem a technickým řešením“.

Jak to ale uděláme? Jakým způsobem se ujistíme o správnosti těchto údajů?

Je to vlastně úplně stejné jako otázka důvěry v dokument, který je elektronicky podepsán (či opatřen elektronickou značkou): i zde budeme vše odvozovat od podpisu (resp. značky) na certifikátu. Bude nás zajímat, zda tato značka je platná – což zase zjistíme podle toho, zda je založena na stále platném systémovém certifikátu. Jeho platnost zase posoudíme podle platnosti značky, kterou je tento certifikát opatřen. A tak dále – vždy musíme nejprve prozkoumat platnost elektronické značky na „nadřazeném" certifikátu.

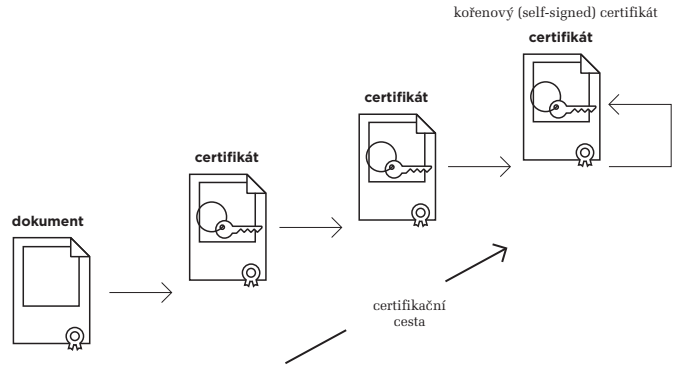
3.5.1 Certifikační cesta

Pokud vám předchozí odstavec připomněl jakýsi bludný kruh, pak je to zcela správně: snaha ověřit platnost podpisu na výchozím dokumentu nás přinutila ze všeho nejdříve prozkoumat jiný podpis (značku). A ještě předtím musíme prozkoumat jiný podpis (značku) atd.

Asi již tušíte, že při takovémto postupu se budeme pohybovat „zdola nahoru" po takové posloupnosti (hierarchicky uspořádaných) certifikátů, kterou jsme si už jednou (v části 1.15) označili jako **certifikační cestu**, viz obrázek.

Obrázek 3-12

Představa certifikační cesty



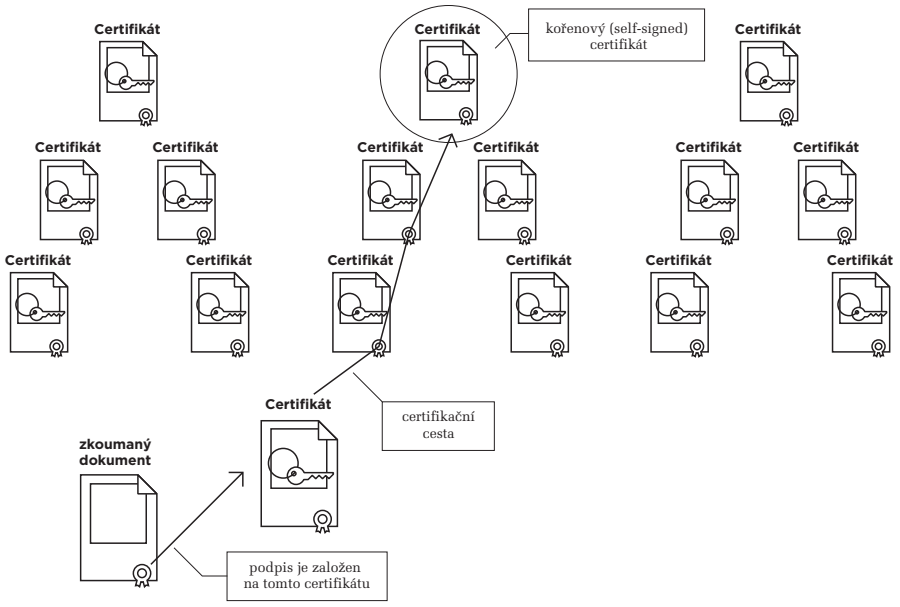
Obrázek naznačuje i opatření, díky kterému není tato certifikační cesta nekonečná: končí u takového certifikátu, který je **podepsán sám sebou** (resp. je certifikátem **s vlastním podpisem**, v angličtině **self-signed**), a tudíž již nemá "nad sebou" žádný nadřazený certifikát.

> Certifikát „podepsaný sám sebou" je podepsaný pomocí soukromého klíče, ke kterému je sám vystaven – a obsahuje tedy ten veřejný klíč, který je s tímto soukromým klíčem do páru. Řečeno jinými slovy: k ověření platnosti elektronické značky na tomto certifikátu se použije veřejný klíč, obsažený přímo v tomto certifikátu.

Připomeňme si také, že certifikační cesta úzce souvisí se **stromy důvěry**, které jsme si popisovali již v první kapitole: certifikační cesta je vlastně jedním možným průchodem takovýmto stromem či lesem, a to směrem „zdola nahoru“ až k některému z kořenů stromu. Přitom každý kořen (kořenový certifikát) musí být již z principu „podepsaný sám sebou“, aby neměl již žádný nadřazený certifikát.

Pro náš účel je přitom důležité to, aby se ze zkoumaného certifikátu (na kterém je založen podpis na našem dokumentu) dalo „vystoupat“ po nějaké certifikační cestě až k některému z kořenových certifikátů (které jsou nutně certifikáty „s vlastním podpisem“).

Obrázek 3-13
Představa hledání certifikační cesty



Nyní si již můžeme jednoduchým způsobem zformulovat požadavek, který se týká ověřování platnosti toho podpisu, který nás primárně zajímá: nejprve musíme ověřit platnost celé certifikační cesty od tohoto certifikátu. Tedy ověřit platnost elektronických značek na všech nadřazených certifikátech, ležících na této cestě. Samozřejmě včetně toho, zda tyto certifikáty nebyly revokovány, zda stále trvá jejich řádná platnost a zda nebyla porušena jejich integrita.

3.5.2 Jak se hledá certifikační cesta?

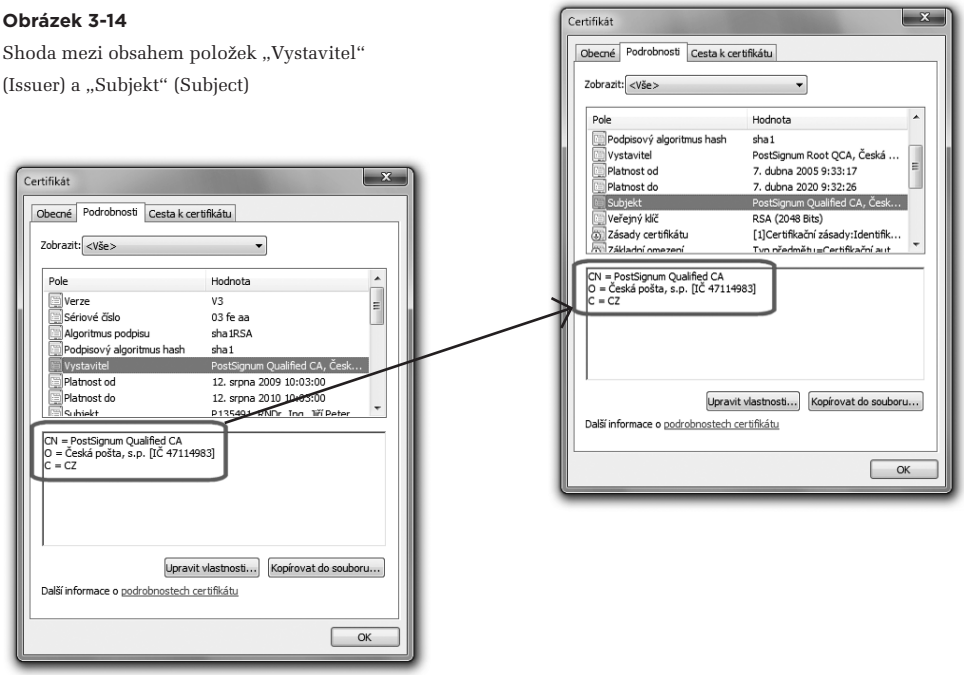
Hledání konkrétních certifikačních cest a ověřování platnosti certifikátů na této cestě je samozřejmě úkolem pro programy, které pracují s elektronickými podpisy, značkami a razítky. Probíhá obvykle automaticky, bez přímého zapojení „lidského“ uživatele. Přesto je ale vhodné přinejmenším vědět, podle jakých pravidel toto hledání probíhá.

Až si budeme v páté kapitole (v části 5.3) podrobněji popisovat vnitřní strukturu dnes používaných certifikátů, zjistíme, že obsahují různé konkrétní položky, podle kterých by hledání certifikačních cest mohlo probíhat. Vodítkem by mohlo být jméno certifikační autority. To bychom měli najít jak na „podřízeném“ certifikátu, tak i na „nadřazeném“ certifikátu. Pochopitelně ale v jiných položkách:

- u „podřízeného“ certifikátu v položce **Vystavitel** (anglicky **Issuer**): zde identifikuje tu certifikační autoritu, která certifikát vydala
- u „nadřízeného“ certifikátu v položce **Subjekt**, či **Předmět** (anglicky **Subject**): zde identifikuje toho, komu certifikát patří, resp. komu byl vystaven. Tedy konkrétní certifikační autoritu.

Příklad „spárování“ dvou konkrétních certifikátů podle jména certifikační autority ukazuje obrázek.

Obrázek 3-14
Shoda mezi obsahem položek „Vystavitel“ (Issuer) a „Subjekt“ (Subject)



Takovéto „párování“ (podle jména certifikační autority) se ale v praxi hodí jen pro prokázání opačného případu: když se hodnoty příslušných položek neshodují, můžeme z toho odvodit, že příslušné certifikáty „neleží vedle sebe“ na stejné certifikační cestě.

Důležité ale je, že opačně to neplatí: obsah obou položek se může shodovat i v případě, kdy nejde o „nadřazený“ a „podřízený“ certifikát. Jedna a tatáž certifikační autorita totiž může podepisovat vydávané (vystavované) certifikáty pomocí různých soukromých klíčů, resp. jejich podpisy mohou

být založeny na různých kořenových certifikátech dané certifikační autority. To se ale při „párování“ jen podle jména certifikační autority nezohlední.

Pro pozitivní ověření vzájemné vazby mezi dvěma certifikáty je proto musíme „spárovat“ podle soukromého klíče, použitého k podepsání „podřízeného“ certifikátu při jeho vystavování.

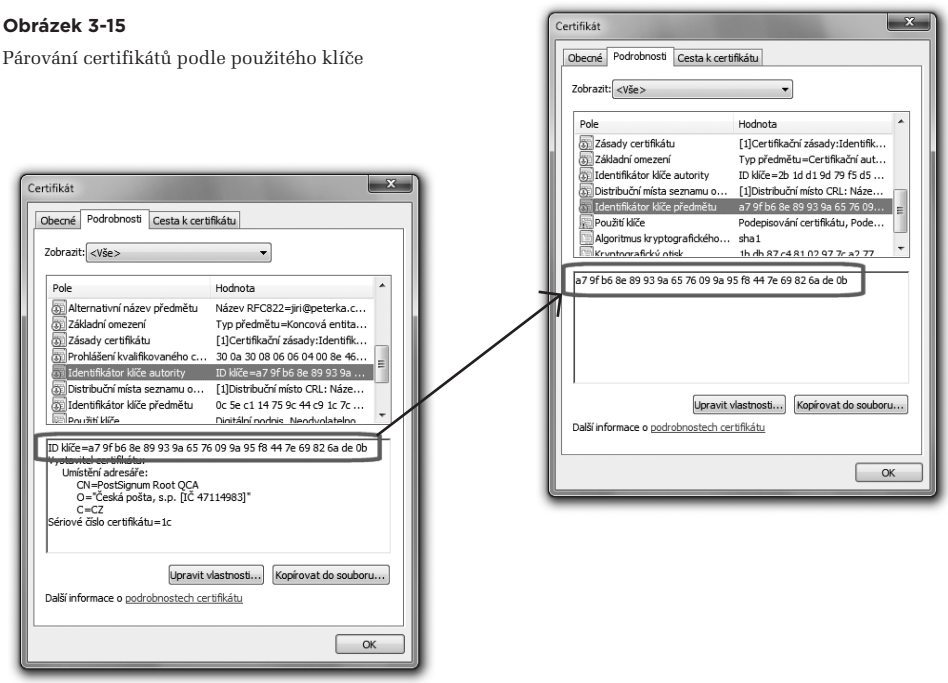
Tento klíč samozřejmě není v žádném z obou certifikátů obsažen, ale najít zde můžeme alespoň jeho jednoznačný identifikátor, který je určitým způsobem odvozen z otisku soukromého klíče. Tento identifikátor bývá obsažen:

- u „podřízeného“ certifikátu v položce **Identifikátor klíče autority (Authority Key Identifier)**
- u „nadřízeného“ certifikátu v položce **Identifikátor klíče předmětu (Subject Key Identifier)**

Příklad „spárování“ dvou konkrétních certifikátů podle identifikátoru klíče vidíte na obrázku.

Obrázek 3-15

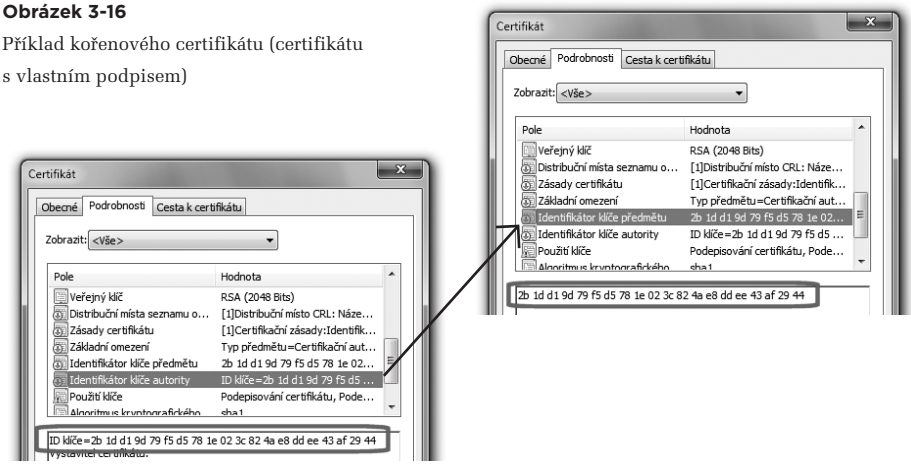
Párování certifikátů podle použitého klíče



(Horní) konec certifikační cesty, který odpovídá kořenovému certifikátu, pak poznáme podle toho, že jde o certifikát s vlastním podpisem. Ten jediný nemusí obsahovat obě popisované položky s identifikátory klíče – ale pokud je obsahuje, shodují se.

Obrázek 3-16

Příklad kořenového certifikátu (certifikátu s vlastním podpisem)



4. Elektronický podpis z pohledu práva

Kapitola 4

4. Elektronický podpis z pohledu práva

V této kapitole se již zaměříme na ty aspekty elektronického podpisu (ale také elektronických značek a časových razítek), které nejsou ani tak technické, jako spíše právní.

Podrobněji si rozvedeme to, s čím jsme se poprvé seznámili již v první kapitole: že není elektronický podpis jako elektronický podpis, ale že elektronických podpisů existuje více druhů. A že hlavní odlišností mezi nimi je to, jak dalece jim můžeme věřit. Zejména pokud jde o identitu podepsané osoby.

V praxi se možná nejvíce hovoří o **zaručeném elektronickém podpisu**, který je ale z pohledu důvěryhodnosti paradoxně „nejslabší". Na opačné škále pak je **uznávaný elektronický podpis**, který je naopak „nejsilnější".

Vedle těchto dvou variant existují ještě další druhy elektronických podpisů, a všechny se mezi sebou liší zejména požadavky na certifikát, na kterém jsou založeny. Proto se podrobněji seznámíme také s problematikou certifikátů. Nejvíce si řekneme o tzv. **kvalifikovaných certifikátech**, na které se můžeme spoléhat nejvíce a které vydávají tzv. **kvalifikovaní poskytovatelé certifikačních služeb**, alias **kvalifikované certifikační autority**.

Nebo jiná otázka, ke které se v této kapitole dostaneme znovu a podrobněji: komu vlastně patří elektronický podpis?

V prvním přiblížení si na ni můžeme odpovědět hned a jednoduše: elektronický podpis patří tzv. **podepisující osobě**, jejíž identita je popsána v certifikátu. V praxi to ale může být složitější, protože přímo v certifikátu nemusí být dostatek údajů na to, abychom podepisující osobu dokázali spolehlivě identifikovat a rozlišit od jiných osob. Takovéto rozlišení je ale velmi podstatné pro toho, kdo pracuje s nějakým elektronickým dokumentem, vyhodnocuje platnost elektronického podpisu (či elektronické značky) na tomto dokumentu a hodlá se spoléhat na výsledek svých zjištění (proto je tzv. **spoléhající se osobou**).

Připomenout si můžeme také „právní" terminologii: ta místo o soukromém a veřejném klíči hovoří o **datech pro vytváření elektronických podpisů**, resp. o **datech pro ověřování elektronických podpisů**. A vedle nich hovoří o **prostředcích pro vytváření elektronických podpisů** a o **prostředcích pro ověřování elektronických podpisů** (což jsou v praxi programy či zařízení, které slouží pro práci s elektronickými podpisy).

Ještě jednou se také vrátíme k problematice dlouhodobého statutu elektronických dokumentů a podíváme se na ni více z pohledu práva, než z pohledu technologie.

4.1 Co není (zaručeným) elektronickým podpisem

Když jsme si v předchozích kapitolách popisovali, jak vzniká elektronický podpis a jak se vyhodnocuje jeho platnost, vybudovali jsme si tím i určitou představu toho, co už je elektronickým podpisem a co ještě nikoli. A třeba představa elektronického podpisu „jako známky" či „jako razítka" nám do této představy nezapadla, protože „naším" elektronickým podpisem je pouze takový, který stojí na principech asymetrické kryptografie, vzniká s využitím soukromého klíče, vyhodnocuje se pomocí veřejného klíče a opírá se o certifikáty, které se zase opírají o existenci celé infrastruktury veřejného klíče.

Nicméně když zákonodárci v EU přijímali výchozí unijní legislativu pro elektronický podpis, nastavili pomyslnou „laťku" podstatně níže. Elektronický podpis definovali „tak nízko" a tak technologicky neutrálně, že by se za něj daly považovat i takové věci, které do naší představy (viz druhá a třetí kapitola) vůbec nezapadají. A nezapadají ani do toho, jak je dnes elektronický podpis v praxi všeobecně vnímán.

Naštěstí i náš zákon[1] vymezuje různé úrovně elektronických podpisů, a ty vyšší již lépe odpovídají realitě. Konkrétně námi vytvořené představě elektronického podpisu odpovídá až tzv. **zaručený elektronický podpis**.

Proto jsme také v první kapitole zavedli úmluvu o tom, že kdykoli řekneme „elektronický podpis" bez dalších upřesnění, budeme tím mít na mysli to, co zákon definuje jako „zaručený elektronický podpis".

Přesto určitě nezaškodí, když si zde podrobněji rozebereme i ty podpisy, které do naší představy elektronického podpisu nezapadají a nejsou ani zaručenými elektronickými podpisy (z pohledu zákona).

Začít musíme od toho, jak je elektronický podpis vymezen v zákoně. Ten jej definuje jako:

> *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.*

Povšimněte si dobře, že zde není uveden žádný požadavek na způsob vzniku podpisu (oněch „údajů v elektronické formě"). Nemusí tedy nutně vznikat způsobem, který jsme si popisovali ve druhé kapitole, s využitím dvojice asymetrických klíčů (soukromého a veřejného) a nějakého certifikátu.

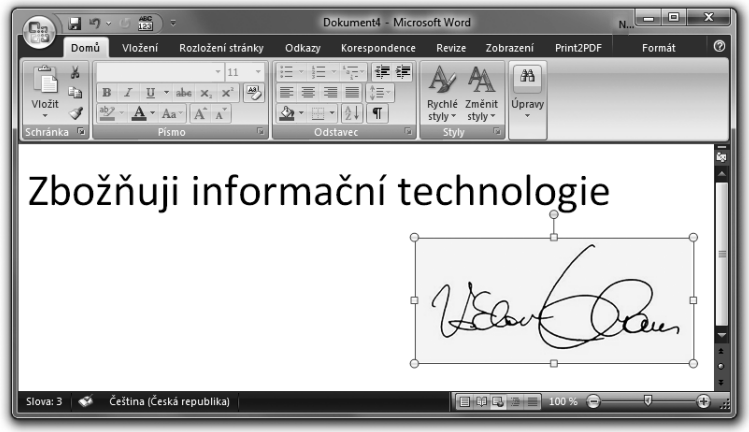
Je zajímavou otázkou, zda by takto vágní definici v zákoně nevyhovělo například to, co jsme si již jednou ukazovali jako příklad toho, co bychom opravdu (ale opravdu) neměli považovat za elektronický podpis: když někde naskenujeme něčí vlastnoruční podpis, z nějakého listinného dokumentu či odjinud, a výsledný obrázek pak pomocí vhodného programu „přilepíme" k nějakému textu.

---

[1] Zákon č. 227/2000 Sb., „o elektronickém podpisu", v platném znění.

Jako na příkladu z části 2.1, kdy autor této knihy sejmul podpis prezidenta Václava Klause, převedl jej do podoby rastrového obrázku (tedy: údajů v elektronické podobě), a následně vložil v textovém editoru k nějakému textu („připojil k datové zprávě“).

Obrázek 4-1
Text s přiloženým snímkem podpisu Václava Klause



Dá se z takovéhoto artefaktu, který může vytvořit skutečně kdokoli, *„jednoznačně ověřit identita podepsané osoby ve vztahu k datové zprávě*“, jak to požaduje zbývající část definice elektronického podpisu?

Kdo zná podpis Václava Klause (nebo se na něj někde podívá), mohl by si v první chvíli skutečně myslet, že uvedený text podepsal Václav Klaus. Tedy identifikovat Václava Klause jako podepsanou osobu. Ale určitě ho velmi rychle napadne otázka, zda takovýto „podpis“ skutečně zachycuje projev vůle podepisující (resp. podepsané) osoby. Můžeme z něj odvozovat souhlas Václava Klause s obsahem podepsaného dokumentu (či zprávy)?

Určitě ne. Stejně tak z něj ale nemůžeme odvozovat ani jeho nesouhlas. Nemůžeme z něj zkrátka odvozovat vůbec nic. Předpokládat nemůžeme ani to, že podpis na předchozím obrázku vytvořil sám Václav Klaus.

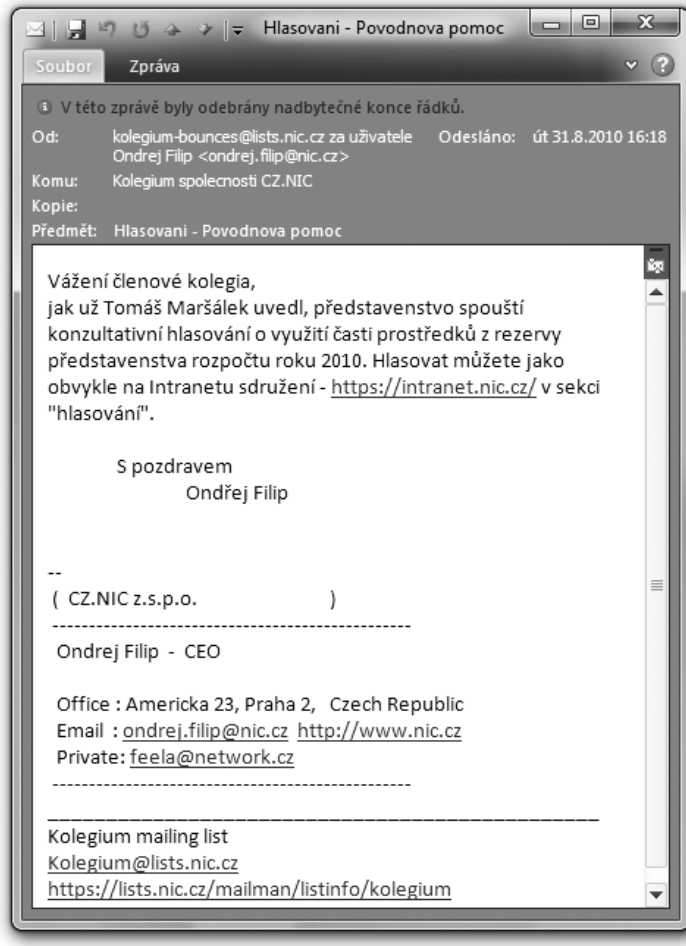
A tady už narážíme na první zásadní problém: definice elektronického podpisu tuto otázku neřeší. Nepožaduje tedy (ani nepřímo) projev vůle podepsané osoby. Možná proto, že řeší jen přívlastek „elektronický“ a nedefinuje základní atributy „podpisu“ jako takového, mezi které by projev vlastní vůle určitě patřit měl.[2]

[2] Atributy (vlastnoručního) podpisu ale také nejsou nikde (v zákoně) definovány.

V každém případě musíme takovýto druh artefaktu odmítnout, resp. vyloučit z toho, co považujeme za elektronický podpis. Zde již pro samotnou absenci projevu vůle podepisující (podepsané) osoby.

Kde již situace nemusí být až tak jasná, jsou nejrůznější „podpisové patičky“ u zpráv elektronické pošty. Mají podobu textu, který se přikládá (buď ručně, častěji ale automaticky) na konec jednotlivých emailů, a obsahuje nejrůznější identifikační údaje o autorovi zprávy. Příklad vidíte na dalším obrázku. V praxi takovéto druhy textových podpisů mohou poskytovat (a často také poskytují) velmi důležité a užitečné informace. Problém je ale v tom, že se na ně nemůžeme spolehnout.

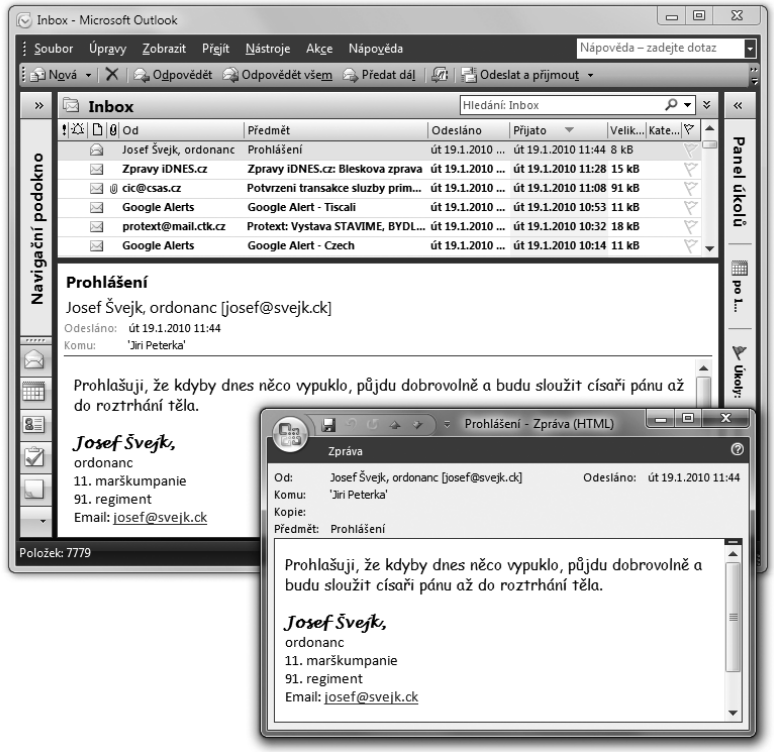
Snad nepřekvapí konstatování, že do takovéto „patičky“ na konci emailové zprávy si může každý napsat, cokoli ho jen napadne. A vůbec se přitom nemusí vydávat za sebe sama.



Obrázek 4-2
Příklad textového podpisu (patičky) na konci emailové zprávy

Pokud chcete příklad, můžete ho vidět na obrázku s emailem od literární postavy Josefa Švejka.[3]

Obrázek 4-3
Email s textovým podpisem literární postavy Josefa Švejka



Je otázkou, zda by takováto „podpisová patička“ vyhověla definici elektronického podpisu, tak jak je obsažena v zákoně. Určitě by ale nevyhověla definici zaručeného elektronického podpisu, která odpovídá našemu (zde používanému) i v praxi obvyklému chápání elektronického podpisu.

Proto se takovýmto „elektronickým podpisům“ (bez přívlastku) v této knížce už dále věnovat nebudeme. Ne že by v praxi neměly smysl a nebyly užitečné – ale proto, že bychom je raději neměli vůbec považovat za elektronický podpis (i když by to zákon možná připouštěl).

Spíše se na ně dívejme jako na určitou informaci, která je nám poskytována bez jakýchkoli záruk.

[3] Jen na okraj: tento mail byl skutečně odeslán a řádně doručen, takže snadno zfalšovat lze i adresu odesilatele, uváděnou v hlavičce zprávy poštovním programem (a ne pouze text v roli podpisu, vloženého do těla zprávy).

4.2 Zaručený elektronický podpis

Mnohem více než elektronický podpis „bez přívlastku“ nás zajímá až zaručený elektronický podpis. Ten už podle svého názvu poskytuje určité záruky – byť tyto se týkají spíše technické stránky (způsobu provedení elektronického podpisu), a nikoli ještě právní stránky.

Ve stručnosti bychom to mohli popsat tak, že zaručený podpis je „podpis, založený na certifikátu“.[4] Konkrétně podpis, který vzniká způsobem popsaným ve 2. kapitole a jehož platnost lze ověřit postupy, popsanými ve 3. kapitole. Tedy s využitím páru asymetrických klíčů (soukromého při samotném podepisování a veřejného při ověřování) a s určením identity podepsané osoby pomocí certifikátu.

Způsob, jakým zaručený podpis vzniká, zaručuje integritu podepsaného dokumentu: jakákoli jeho změna (provedená po podpisu) by se při jeho vyhodnocování projevila porušenou integritou. Stejně tak tento druh podpisu umožňuje, aby podepisující osoba mohla držet svůj soukromý klíč výlučně pod svou kontrolou (a nemusela ho dávat nikomu jinému). To proto, že soukromý klíč je zapotřebí pro podepisování, ale nikoli již pro ověřování platnosti podpisu.

Veřejný klíč, obsažený v certifikátu, pak umožňuje každému přesvědčit se, že podpis mohl vytvořit jen ten, kdo měl ve svém držení soukromý klíč. A díky údaji o identitě, který je obsažen v certifikátu, je možné „ukázat prstem“ na toho, kdo má ve svém držení soukromý klíč a měl by tudíž být podepisující, resp. podepsanou osobou.

Schválně si to srovnejme s požadavky, které na zaručený elektronický podpis klade zákon. Ať vidíme, zda jsou či nejsou splněny:

> *zaručeným elektronickým podpisem [se rozumí] elektronický podpis, který splňuje následující požadavky:*
>
> 1. *je jednoznačně spojen s podepisující osobou,*
> 2. *umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,*
> 3. *byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,*
> 4. *je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat*

První dva požadavky odpovídají tomu, že můžeme „ukázat prstem“ na někoho (identifikovat ho) a tvrdit o něm či o ní, že je podepisující (resp. podepsanou) osobou. Třetí požadavek hovoří o tom, že k podpisu stačí soukromý klíč (který si podepisující osoba může nechat jen pro sebe). Čtvrtý požadavek se týká zajištění integrity dat.

---

[4] Ve skutečnosti to může být i jiný druh podpisu – ale požadavkům, kladeným na zaručený elektronický podpis, dnes vyhovuje pouze „podpis, založený na certifikátu“.

Všechny tyto požadavky jsou tedy naším „podpisem, založeným na certifikátu“, splněny.

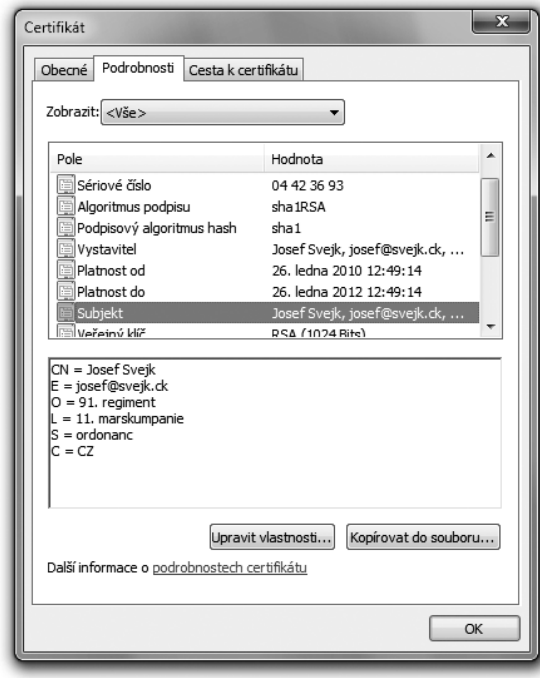
Povšimněme si ale, že zde chybí jeden důležitý požadavek: aby ten, na koho „ukážeme prstem“ (koho identifikujeme jako podepsanou osobu) skutečně existoval a byl skutečně tím, kdo podpis vytvořil.

Jinými slovy: u zaručeného elektronického podpisu sice máme záruku ohledně integrity podepsaného dokumentu, ale nemáme záruku toho, zda „ukazujeme prstem“ na správnou osobu (jako podepsanou osobu).

Ukažme si to na stejném příkladu jako v části 1.5, se zaručeným elektronickým podpisem literární postavy Josefa Švejka. Samozřejmě k tomu budeme potřebovat také certifikát, vystavený na tuto osobu.

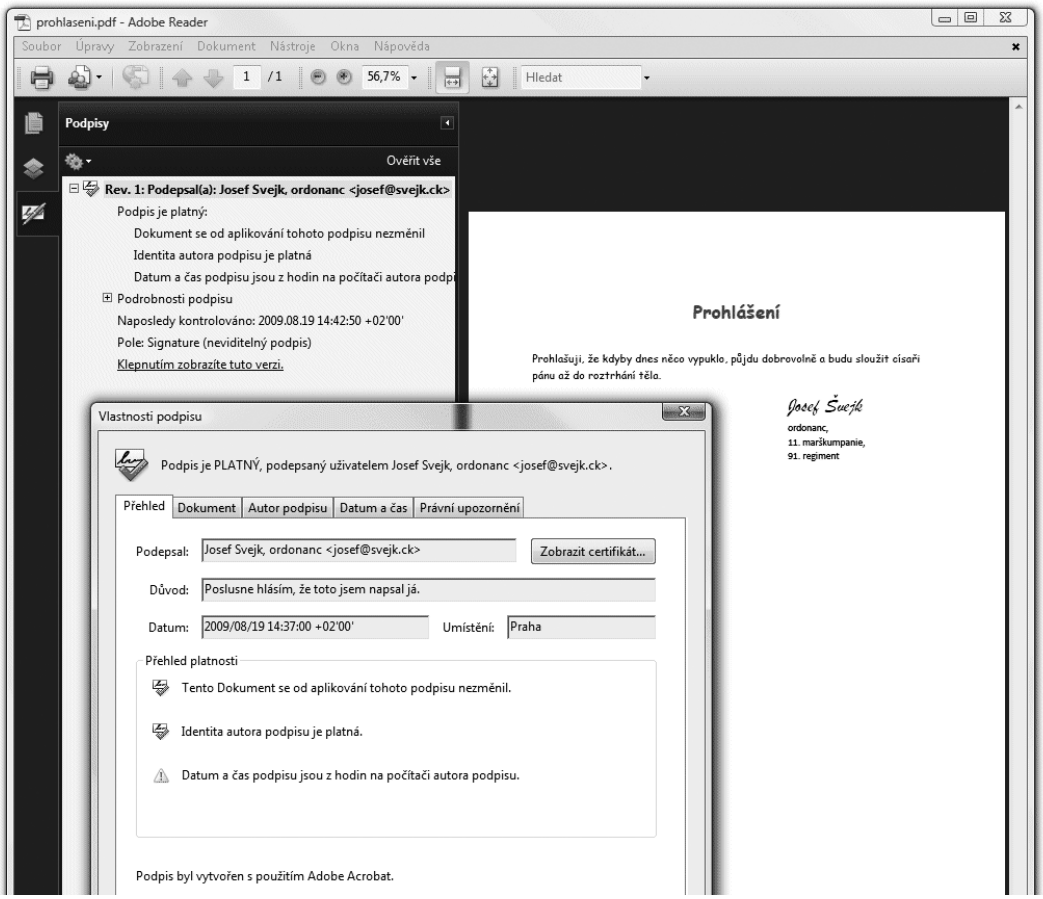
Příklad takového certifikátu ukazuje následující obrázek: podpis, založený na takovémto certifikátu, už je zaručeným elektronickým podpisem. Zajišťuje tedy integritu podepsaného dokumentu, umožňuje podepisující osobě udržet soukromý klíč pod svou kontrolou a umožňuje i identifikaci podepsané osoby: můžeme „ukázat prstem“ na literární postavu Josefa Švejka.

Obrázek 4-4
Příklad certifikátu, znějícího na literární postavu Josefa Švejka



Obrázek 4-5

Příklad platného zaručeného elektronického podpisu (literární postavy) Josefa Švejka



Jistě ale není těžké nahlédnout, že Josef Švejk (coby literární postava) ve skutečnosti neexistuje (jako fyzická osoba) a nemůže tedy být autorem zde prezentovaného zaručeného elektronického podpisu.

To nám jen dokládá, že (pouhý) zaručený elektronický podpisu ještě nemůže být právně závazný a postavený na roveň vlastnoručnímu podpisu. Jeho „zaručenost“ zahrnuje pouze zajištění integrity podepsaného dokumentu: platný zaručený elektronický podpis nám dává jistotu, že dokument se od svého podepsání nezměnil. Už nám ale nedává jistotu ohledně toho, komu podpis patří, resp. kdo jej vytvořil a je podepsanou osobou.

4.2.1 Co schází zaručenému elektronickému podpisu?

To, co brání (pouhému) zaručenému elektronickému podpisu v tom, aby spolehlivě vypovídal i o podepsané osobě – a tato nemohla popřít, že podpis vytvořila – je „kvalita" certifikátu. Přesněji: požadavek, který by se týkal pravdivosti a hodnověrnosti toho, co je v certifikátu obsaženo. Zde, v příkladu s literární postavou Josefa Švejka, jsme uvěřili obsahu certifikátu, který byl vystaven literární postavě Josefa Švejka – a pak nám zákonitě vyšlo, že podpis „patří" postavě Josefa Švejka.

Takovýto certifikát si ale může vystavit skutečně kdokoli, třeba i „na koleně". Stačí k tomu umět si na svém počítači spustit jednoduchý program (dostupný i jako freeware) a tomu zadat to, co chceme mítv certifikátu napsáno.

Teď si zkuste představit, že by si někdo takto vyrobil certifikát nikoli na literární postavu Josefa Švejka, ale na vaše jméno a vaší identitu. Pak by mohl vytvářet zaručené elektronické podpisy, které by vypadaly jako „vaše vlastní". Určitě byste ale nechtěli nést právní následky toho, co by někdo jiný takto podepsal za vás.

Naštěstí byste ani nemuseli. Zaručený elektronický podpis nemůže být právně závazný už jen proto, že podepsaná osoba může kdykoli popřít, že by takový podpis kdy vytvořila. Chybí mu totiž jeden z důležitých atributů, kterým je tzv. **nepopiratelnost**.[5] Tu zákon od (pouhého) zaručeného podpisu skutečně nepožaduje. Požaduje ji až od vyšších forem elektronického podpisu, které již jsou založeny na kvalifikovaném certifikátu.

Problém u předchozího příkladu s podpisem literární postavy Josefa Švejka byl v tom, že tento podpis nebyl založen na kvalifikovaném certifikátu. Proto ani neumožňuje věrohodně ověřit, zda dokument skutečně podepsal Josef Švejk. Nebo, z opačného pohledu: neumožňuje vyloučit, že podpis ve skutečnosti vytvořil někdo jiný. Což se ale právě zde stalo.

4.3 Certifikáty, certifikační autority a certifikační politiky

Pokud budeme požadovat právní závaznost elektronických podpisů a jejich srovnatelnost s vlastnoručními podpisy na listinných dokumentech, budeme potřebovat takové certifikáty, které jsou dostatečně důvěryhodné a současně jsou vhodně „ukotveny v zákoně", aby se z nich daly odvozovat právní důsledky. A to jsou právě (a pouze) **certifikáty kvalifikované**. Ty mohou vydávat pouze takové certifikační autority, které jsou samy kvalifikované (tj. jsou to **kvalifikovaní poskytovatelé certifikačních služeb**) a tudíž samy splňují požadavky, kladené na ně zákonem.

Abychom tomu ale správně rozuměli: toto konstatování rozhodně neznamená, že by všechny ostatní certifikáty (tj. nikoli kvalifikované) byly apriorně nedůvěryhodné a nedaly se využít k žádnému účelu.

---

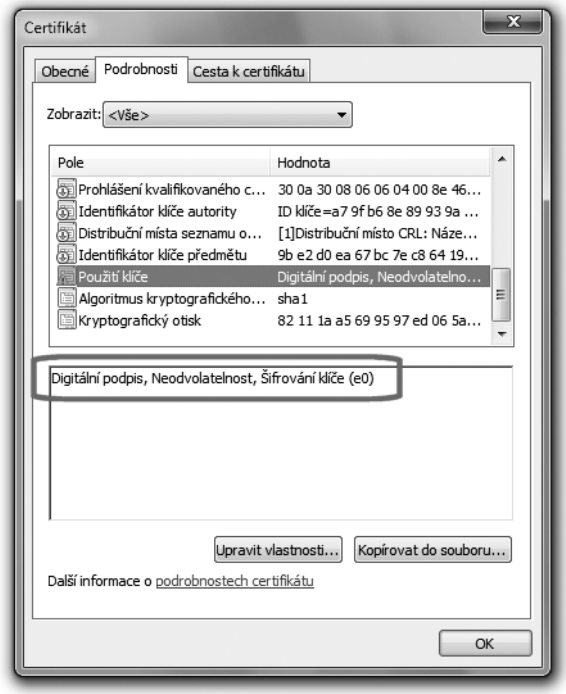
[5] Ve smyslu nepopiratelné odpovědnosti, resp. nemožnosti popřít odpovědnost, viz kapitola 1.

4.3.1 Účely certifikátů

Certifikáty se v praxi používají pro řadu různých účelů a nikoli pouze pro podepisování dokumentů (v právním slova smyslu). Používají se také pro šifrování dat nebo klíčů, k identifikaci a autentizaci (při přihlašování k nějakému informačnímu systému), pro zabezpečenou komunikaci prostřednictvím protokolů SSL/TLSapod.

Někdy jsou podle těchto účelů jednotlivé druhy certifikátů pojmenovány: hovoří se o **certifikátech podpisových** (používaných pro podepisování), **certifikátech serverových** (kterými se servery identifikují vůči svým klientům), **certifikátech emailových** (kterými se zabezpečuje elektronická pošta), **certifikátech pro šifrování** atd. Někdy (jako například u podpisových certifikátů) však jde jen o neformální označení, používané například v médiích či v rámci marketingu. Jindy (jako třeba u serverových certifikátů) ale již jde o pojmenování, které používají samotné certifikační autority.

Správně jsou ale účely, ke kterým je možné konkrétní certifikát využít, určeny jinak a mnohem přesněji, než neformálním pojmenováním certifikátu. Navíc nejde ani tak o účely vztahující se k certifikátu jako takovému, jako k jeho „párovým datům“ (tj. k veřejnému klíči, který je v certifikátu obsažen, a k soukromému klíči, který je s tímto certifikátem spojen). Přesto se o nich hovoří jako o „účelech certifikátu“.



Obrázek 4-6
Příklad účelů (možných použití klíče), specifikovaných přímo v certifikátu

Po právní stránce platí, že každá certifikační autorita stanovuje při vydávání svých certifikátů, k jakým účelům mohou být využity. Tyto účely pak jsou v samotném certifikáty explicitně vyjmenovány, v rámci k tomu určené položky (příklad viz předchozí obrázek).

V případě kvalifikovaných certifikátů má ale certifikační autorita svázané ruce, protože zde jí přípustné účely stanovuje zákon.[6] A ten říká, že kvalifikované certifikáty lze využít jen pro účely podepisování dokumentů[7] a k ničemu jinému.

Volnou ruku má certifikační autorita až u volby účelů, ke kterým smí být využity ostatní druhy certifikátů (které zahrnujeme pod společný zastřešující pojem komerční certifikáty, viz dále). U nich již nejsou účely jejich využití zákonem omezeny. Můžeme je tedy použít i pro podepisování dokumentů, ale neměli bychom to dělat z jiného důvodu.

Chceme-li totiž, aby náš podpis měl právní relevanci (a jím podepsaný elektronický dokument byl rovnoprávný s vlastnoručně podepsaným listinným dokumentem), stejně musíme použít certifikát kvalifikovaný.

4.3.1.1 Kritické a nekritické účely

Každý program, který pracuje s nějakým certifikátem, resp. s jeho párovými daty (soukromým či veřejným klíčem), by měl vycházet z toho, jaké účely jsou uvedeny přímo v samotném certifikátu.

Zde připadají v úvahu dvě možnosti, neboť jednotlivé účely zde mohou být uvedeny:

- jako „povinné“ (tzv. kritické), které je nutné dodržet
- jako „nepovinné“ (tzv. nekritické), které jsou pouze doporučené a není nutné je dodržet.

Již kvůli existenci nekritických účelů ale musí být volba účelů znovu řešena i na úrovni jednotlivých programů. Jinými slovy: každý program, který s certifikáty (resp. s jejich párovými daty) pracuje, si může znovu definovat výčet účelů, ke kterým se konkrétní certifikát může použít.

Správně by tyto účely měly korespondovat s účely, které jsou uvedeny přímo v certifikátu, ale někdy tomu tak nebývá a uživatel si u každého certifikátu může nastavit takové účely, jaké uzná za vhodné. Může tím ale porušit podmínky pro používání certifikátu, které se při jeho vystavení zavázal dodržovat (viz dále).

---

6 Přesněji vyhláška č. 378/2006 Sb., která se odkazuje na normu ČSN ETSI TS 101 456 (a ta zakazuje použití párových dat pro jiné účely, než je podepisování dokumentů).

7 Ještě přesněji jen pro takové podepisování, při kterém se podepisující osoba seznamuje s obsahem podepisovaného dokumentu. K tomu nedochází v případě autentizace (prokazování identity), kdy je podepisován automaticky generovaný kontrolní údaj, se kterým se autentizující osoba neseznamuje. Proto kvalifikovaný certifikát nesmí být využit ani pro autentizaci.

Obrázek 4-7
Volba účelů při vkládání kořenového certifikátu certifikační autority do úložiště certifikátů prohlížeče Firefox

Jiným důvodem pro možnost volby účelů ještě na úrovni jednotlivých programů je specifičnost toho, k čemu tyto programy chtějí certifikáty používat. Jsou to účely, které mohou být vymezeny mnohem detailnější než ty, které jsou rozlišovány a uváděny přímo v certifikátu.

4.3.2 Certifikační politiky

Připomeňme si, že pro kvalifikované certifikáty jsou jejich náležitosti definovány v zákoně.[8] To platí i pro účely, ke kterým mohou být kvalifikované certifikáty využity (jde jen o podepisování dokumentů). Stejně tak jsou zákonem definovány i požadavky na činnost kvalifikovaných poskytovatelů certifikačních služeb, kteří takovéto kvalifikované certifikáty vydávají.

Zákony ale definují jen ty nejzásadnější a nejdůležitější požadavky na kvalifikované certifikáty a jejich vydavatele. Jako třeba to, že kvalifikovaný certifikát má obsahovat jméno a příjmení podepisující osoby, i jméno či označení svého vydavatele.

Řada dalších rozhodnutí, která již nejsou tak zásadní – a která se týkají jak vlastností certifikátů, tak i postupů při jejich vydávání – je již ponechána na rozhodnutí samotných poskytovatelů certifikačních služeb. Ti si například sami rozhodují o tom, jaký konkrétní postup budou požadovat při identifikaci žadatele o vydání kvalifikovaného certifikátu, jaké doklady totožnosti po něm budou vyžadovat atd. Nebo třeba to, s jakou platností budou své certifikáty vydávat atd.

Všechna tato rozhodnutí jsou zanesena do **tzv. certifikačních politik**. To jsou dokumenty, ve kterých jednotliví poskytovatelé přesně a detailně popisují podmínky a postupy při vydávání svých certifikátů, možnosti a způsoby jejich využití a další důležité skutečnosti, týkající se například možností revokace atd.[9]

[8] V zákoně č. 227/2000 Sb., o elektronickém podpisu, v platném znění.

[9] Základní požadavky na tyto certifikační politiky jsou definovány ve vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Tyto certifikační politiky jsou přitom odlišné pro různé druhy certifikátů, které jedna a táž certifikační autorita (poskytovatel certifikačních služeb) vydává. Takže v praxi certifikační autorita obvykle má samostatnou certifikační politiku pro vydávání každého jednotlivého druhu certifikátu ze své nabídky.

> Například: kořenová certifikační autorita PostSignum (PostSignum Root QCA) má jednu certifikační politiku, podle které vydává kvalifikované certifikáty svým podřízeným certifikačním autoritám.
>
> Kvalifikovaná certifikační autorita PostSignum (PostSignum QCA, podřízená kořenové certifikační autoritě) má dvě certifikační politiky: jednu pro vydávání kvalifikovaných osobních certifikátů a jednu pro vydávání kvalifikovaných systémových certifikátů.
>
> Komerční certifikační autorita PostSignum (PostSignum VCA, podřízená kořenové CA) má tři certifikační politiky: jednu pro vydávání komerčních osobních certifikátů, jednu pro vydávání komerčních serverových certifikátů a jednu pro vydávání certifikátů pro šifrování.

Každý zákazník, kterému je vydáván nějaký certifikát, pak musí být nejprve seznámen s příslušnou certifikační politikou a následně potvrdit (podpisem na smlouvě o vydání certifikátu), že s certifikační politikou souhlasí. Je to nutné také proto, že v certifikační politice jsou definovány některé základní vztahy mezi poskytovatelem certifikačních služeb (certifikační autoritou) a zákazníkem. Například pokud jde o odpovědnost poskytovatele služeb (za co ručí a za co ne), o účely certifikátu (k čemu smí být využit a k čemu ne), o povinnostech zákazníka (co smí a co nesmí), o možnostech revokace (předčasného zneplatnění certifikátu) atd.

4.3.3 Osobní vs. systémové certifikáty

Jedním z konkrétních důsledků, které by měly vyplývat již z požadavků zákona, je to, že kvalifikovaný certifikát by nikdy neměl být vystaven neexistující fyzické osobě. Tudíž ani literární postavě Josefa Švejka (například). A naopak: je-li nějaký certifikát kvalifikovaný, pak mohl být vydán jen existujícímu subjektu.

Zde už ale neplatí, že se nutně musí jednat o fyzickou osobu, a tedy o „osobní“ kvalifikovaný certifikát. Vzhledem k zavedení elektronických značek, ale i časových razítek, je možné vystavovat kvalifikované certifikáty i jiným subjektům. Hlavně právnickým osobám, organizačním složkám státu atd.

Aby se tyto dvě varianty kvalifikovaných certifikátů vhodně odlišily od sebe, zavedlo se jejich dělení na osobní a systémové:

- **kvalifikované osobní certifikáty** se vystavují pouze reálně existujícím fyzickým osobám, ať již jsou zaměstnanci organizací, podnikajícími fyzickými osobami (OSVČ) nebo nepodnikajícími fyzickými osobami
- **kvalifikované systémové certifikáty** se mohou vystavovat jak fyzickým osobám (podnikajícím i nepodnikajícím), tak i právnickým osobám a organizačním složkám státu.

Jak je z uvedeného členění patrné, i kvalifikovaný systémový certifikát může být vystaven fyzické osobě. Charakter subjektu, kterému je certifikát vystaven, proto není správnou dělicí čárou mezi oběma variantami. Přívlastek „osobní“ u první varianty je proto poněkud zavádějící.

Správným rozlišujícím kritériem mezi osobními a systémovými (kvalifikovanými) certifikáty je jejich možné využití (účel): osobní certifikáty se používají v souvislosti s elektronickými podpisy (tj. elektronické podpisy jsou založeny na osobních certifikátech), zatímco ty systémové se používají v souvislosti s elektronickými značkami a časovými razítky (tj. elektronické značky a časová razítka jsou založena na systémových certifikátech).

U obou variant kvalifikovaných certifikátů ale platí, že požadavky na ně (i na jejich vydavatele) definuje zákon. A ten mj. předepisuje jejich vydavateli (kvalifikovanému poskytovateli certifikačních služeb) velmi důkladně identifikovat ten subjekt, kterému kvalifikovaný certifikát vydává. Jak konkrétně pak vydavatel tento požadavek realizuje, už je specifikováno v příslušné certifikační politice.

4.3.4 Kvalifikované vs. komerční certifikáty

Rozdělování certifikátů na „osobní“ a „systémové“ se ale používá jen u certifikátů kvalifikovaných.

> Připomeňme si, že všechny ostatní certifikáty obecně označujeme jako **komerční certifikáty**.

Hlavní smysl komerčních certifikátů je možnost jejich nasazení všude tam, kde nepřipadá v úvahu nasazení certifikátů kvalifikovaných. Jak již víme, kvalifikované certifikáty lze využívat jen při podepisování (vytváření elektronických podpisů), při označování (vytváření elektronických značek), resp. při „razítkování“ (vytváření časových razítek).

Vzhledem ke komplementárnosti účelu (jiné účely než podepisování) už ale není možné rozdělovat komerční certifikáty podle stejného kritéria, jako certifikáty kvalifikované, tedy podle využití pro podpis či pro značku/razítko.

Místo toho jsou komerční certifikáty děleny více ad-hoc způsobem, opět ale v závislosti na svém využití. Obvykle na:

- **komerční osobní certifikáty:** jsou vystavovány pouze fyzickým osobám a mohou být použity například pro šifrování, autentizaci, ale třeba i podepisování
- **komerční serverové certifikáty:** mohou být vystavovány jak fyzickým osobám, tak i právnickým osobám či organizačním složkám státu. Používají se zejména pro identifikaci a autentizaci webových serverů vůči jejich klientům, a pro zabezpečenou komunikaci mezi klienty a servery pomocí protokolu SSL/TLS

Některé certifikační autority nabízí například také komerční šifrovací certifikáty, určené právě a pouze pro šifrování.[10]

Zajímavé je, že samotný pojem „komerční certifikát“ v zákonech nenajdeme. Není zde použit, a je zaveden až praxí (právě jako doplněk k pojmu „kvalifikovaný certifikát“).

Zákon[11] definuje pouze kvalifikovaný certifikát. Činí tak ve dvou krocích, když nejprve říká, že:

> *certifikátem [se rozumí] datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu*

a poté již definuje požadavky kladené na kvalifikovaný certifikát, byť nejprve odkazem:

> *kvalifikovaným certifikátem [se rozumí] certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb*

Teprve zmíněný paragraf 12 pak přináší samotné požadavky, kladené na kvalifikovaný certifikát. Ten mimo jiné musí:

- mít v sobě napsáno, že je vydán jako kvalifikovaný
- identifikovat toho, kdo ho vydal
- identifikovat toho, komu byl vydán (a to na úrovni: jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym
- obsahovat veřejný klíč (data pro ověřování podpisu)
- být označen elektronickou značkou poskytovatele certifikačních služeb, ta musí být sama založena na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává
- obsahovat unikátní (sériové) číslo kvalifikovaného certifikátu
- obsahovat údaj o počátku a konci platnosti kvalifikovaného certifikátu

Kromě toho kvalifikovaný certifikát může:

- obsahovat údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu (toho, co je podepisováno) jen pro určité použití,
- obsahovat zvláštní znaky podepisující osoby (vyžaduje-li to účel kvalifikovaného certifikátu – například u tzv. zaměstnaneckých certifikátů údaj o zaměstnavateli)
- obsahovat omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

---

10 Důvodem pro odlišení šifrovacích (komerčních) certifikátů od ostatních komerčních certifikátů jsou i odlišné možnosti nakládání s příslušnými soukromými klíči: u šifrovacích certifikátů mohou být příslušné soukromé klíče svěřeny do úschovy třetí osobě (aby se v případě potřeby dostala k zašifrovaným datům), zatímco u komerčních certifikátů používaných pro autentizaci toto nepřipadá v úvahu (aby se třetí osoba – byť jen v případě potřeby – autentizovala pomocí cizího soukromého klíče a odpovídajícího certifikátu).

11 Zákon č. 227/2000 Sb. o elektronickém podpisu, v platném znění.

Další osobní údaje pak smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby. Zde se může jednat například o emailovou adresu, která se dnes do kvalifikovaných certifikátů běžně vkládá. Nebo třeba údaje o bydlišti držitele certifikátu apod.

4.3.5 Proč je nutné používat komerční certifikáty?

Vraťme se ale ještě k tomu, proč se kvalifikované certifikáty nesmí používat pro jiné účely, než ty které souvisí s podepisováním (či vytvářením značek nebo razítek). Přesněji: proč se přitom nesmí používat soukromé klíče, které jsou s kvalifikovanými certifikáty spojeny. Důvody jsou jak formální, tak i ryze praktické.

Jak uvidíme v kapitole 8, třeba při běžném přihlašování (k nějaké službě či serveru) prostřednictvím certifikátu posílá protistrana přihlašujícímu se uživateli určitou výzvu, kterou uživatel podepíše (aniž by ji vlastně vůbec viděl) a vrací zpět, čímž se vůči protistraně autentizuje (prokazuje svou totožnost). Nekorektně se chovající protistrana by ale mohla přihlašujícímu se uživateli podstrčit (v roli výzvy) otisk prakticky libovolného dokumentu – a pokud by uživatel právě používal kvalifikovaný certifikát, získala by jeho platný (a právě závazný) podpis na tomto dokumentu.

Nebo jiný příklad, související se šifrováním: když si zašifrujete nějaká svá data, určitě si budete chtít někde nechat v záloze kopii (soukromého) klíče, který potřebujete pro dešifrování. Případně ho může chtít do zálohy i váš zaměstnavatel. V některých zemích ho dokonce může požadovat i stát.[12] Pak je ale zásadní rozdíl mezi tím, zda se jedná o komerční certifikát a s ním související soukromý klíč (který nevytváří právně závazné podpisy) nebo o kvalifikovaný certifikát a s ním související osobní klíč (se kterým se již lze platně podepisovat).

Využití kvalifikovaných certifikátů pro jiné účely než přímo související s podepisování zapovídá i zákon č. 227/2000 Sb., o elektronickém podpisu. Ve svém §5 totiž ukládá povinnost nakládat se soukromými klíči tak, aby nemohlo dojít k jejich neoprávněnému použití. Tím nemusí být jen odcizení a následné využití soukromého klíče někým jiným, ale i jeho využití oprávněným vlastníkem pro jiné účely, než je samotné podepisování.

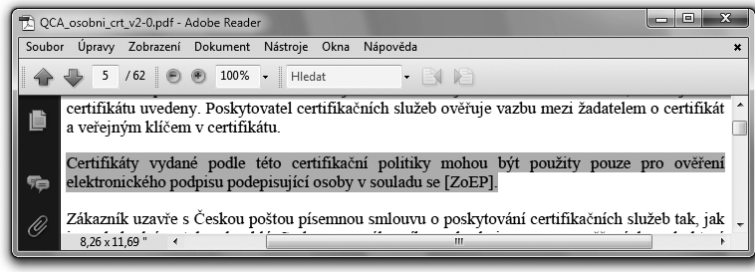
> Povšimněme si také, že zákon formálně hovoří o „datech pro vytváření elektronických podpisů“ a nikoli o soukromém klíči. Tím jakoby zdůrazňuje, že nejde o „univerzálně použitelný“ klíč, ale jen o něco, co se dá využít pouze pro účely vytváření podpisů.

Požadavky zákona (ale i relevantních standardů)[13] se pak odráží i v požadavcích certifikačních autorit, vydávajících kvalifikované certifikáty, formulovaných v jejich certifikačních politikách i obchodních podmínkách.

---

[12] Toto již platí například ve Velké Británii, kde stát má právo požadovat klíč po každém, kdo si něco zašifroval. Za neposkytnutí takovéhoto klíče padly v roce 2010 už i první tresty.

Obrázek 4-8
Výňatek z certifikační politiky CA PostSignum pro vydávání kvalifikovaných certifikátů



4.3.6 Jak se pozná kvalifikovaný certifikát?

Zajímavou otázkou je určitě i to, jak se vlastně pozná kvalifikovaný certifikát. Principiální odpověď vyplývá již z toho, co jsme si vyjmenovali v předchozím odstavci: kvalifikovaný certifikát musí mít v sobě napsáno, že je kvalifikovaný.

V praxi to ale na první pohled – při obvyklém zobrazení certifikátu prostředky operačního systému či právě používané aplikace – nemusí být patrné. Naznačují to ostatně i obrázky na následující stránce: na tom levém je již dříve využitý certifikát literární postavy Josefa Švejka, tak jak ho ukazují standardní prostředky MS Windows. Na pravém obrázku pak je certifikát autora této knihy.

Explicitní informaci o tom, zda jde či nejde o kvalifikovaný certifikát, při tomto pohledu nevidíte. Leccos si ale můžete domyslet: certifikát Josefa Švejka je certifikátem tzv. s vlastním podpisem (self-signed), u kterého se shoduje ten, komu byl vystaven, s tím, kdo ho vystavil (vydal). Tudíž je vyloučeno, aby tento certifikát byl kvalifikovaný. Naproti tomu certifikát na pravém obrázku byl vydán certifikační autoritou PostSignum QCA (Qualified CA) a může tedy být kvalifikovaný.

Jednoznačnou informaci o tom, zda certifikát je kvalifikovaný, ale najdeme až „uvnitř“ certifikátu, pohledem do jeho vnitřních položek (konkrétně do položky „Zásady certifikátu“).

Nejsnáze se k hledanému obsahu dostaneme přes tlačítko „Prohlášení vystavitele“, viz obrázek. Jeho vysvícení (či naopak nevysvícení) také může být určitým vodítkem, ale rozhodující je právě až text, který se zobrazí jako toto prohlášení vystavitele.

Pozor ale na to, že opačný případ se takto nepozná: pokud certifikát není kvalifikovaný, není v něm nikde uvedeno něco jako „tento certifikát není kvalifikovaný“.[14]

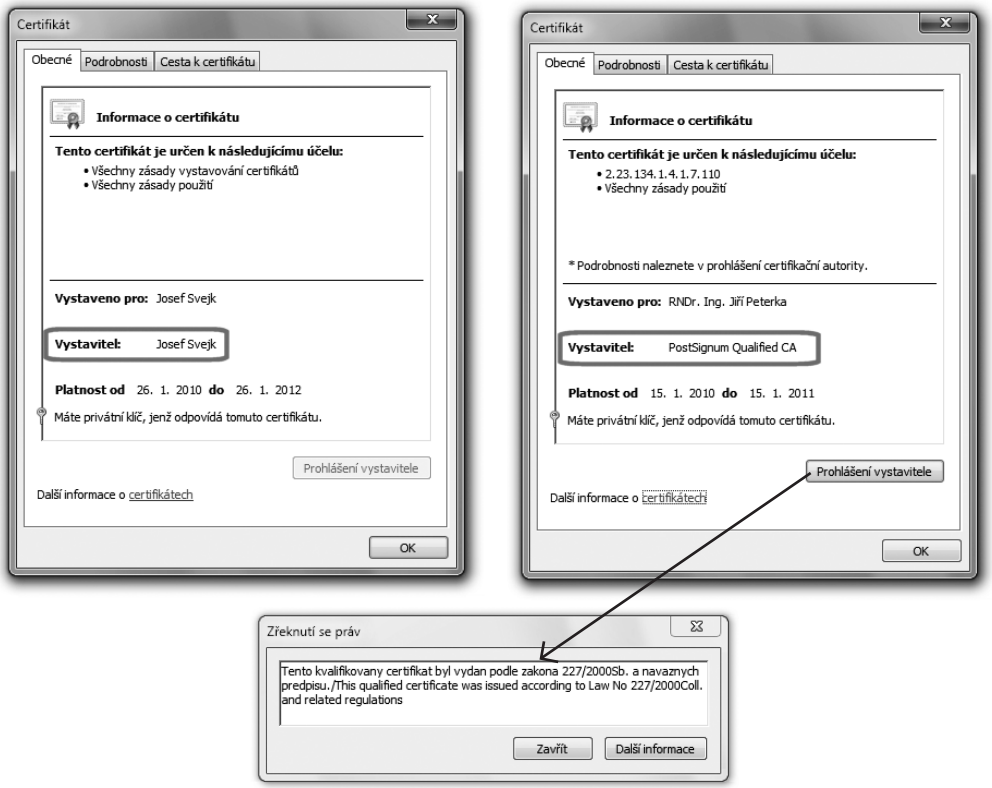
---

13 Konkrétně standardu ETSI TS 101 456 – Electronic Signatures and Infrastructures (ESI) – Policy requirements for certification authorities issuing qualified certificates

14 Stejně tak si ale musíme dát pozor na to, že konstatování o kvalifikovaném charakteru si do svého certifikátu (nejspíše s vlastním podpisem) může napsat kdokoli sám. Takže správně musíme ještě zkontrolovat, zda certifikát vydal kvalifikovaný poskytovatel (tj. poskytovatel, který oznámil, že vydává kvalifikované certifikáty).

Obrázek 4-9

Příklad dvou certifikátů, z nichž pouze jeden je kvalifikovaný



4.4 Zaručený elektronický podpis, založený na kvalifikovaném certifikátu

Vraťme se nyní zpět k různým variantám elektronických podpisů. Vyšším stupněm elektronického podpisu, než je zaručený elektronický podpis, je **zaručený podpis, založený na kvalifikovaném certifikátu.** Jak už vyplývá přímo z jeho označení, od „obyčejného“ zaručeného elektronického podpisu se liší právě v požadavku na certifikát: ten musí být kvalifikovaný.

Jak již víme, kvalifikovaný certifikát je označován jako „kvalifikovaný“ právě proto, že jsou na něj kladeny vyšší požadavky. Dokonce takové, které jsou vymezeny přímo v zákoně (viz předchozí odstavec).

> Tím pádem u tohoto druhu podpisu již nepřipadají v úvahu příklady toho typu, jaké jsme si ukazovali v souvislosti s literární postavou Josefa Švejka: té by nikdy neměl být vystaven kvalifikovaný certifikát.

Díky využití kvalifikovaného certifikátu je tak i příslušný elektronický podpis (tedy: zaručený elektronický podpis, založený na kvalifikovaném certifikátu) výrazně důvěryhodnější. Přesto se v praxi objevují další požadavky na zvýšení celkové důvěryhodnosti těch zaručených podpisů, které jsou založeny na kvalifikovaném certifikátu.

Tyto další požadavky se obecně mohou ubírat dvěma směry:

- cestou dalších požadavků na vydavatele kvalifikovaných certifikátů
- cestou dalších požadavků na vytváření (a ověřování) zaručených elektronických podpisů, založených na kvalifikovaných certifikátech

Praktický rozdíl je pak v tom, že u první varianty je požadována akreditace toho, kdo kvalifikované certifikáty vydává: příslušný poskytovatel certifikačních služeb (certifikační autorita) musí být nejen kvalifikovaný, ale musí také úspěšně projít procesem **akreditace** (tj. **být akreditovaný**).

> O zaručených elektronických podpisech, které jsou založeny na kvalifikovaných certifikátech od takovéhoto poskytovatele, který je akreditován, se hovoří jako o **uznávaných elektronických podpisech** (podrobněji viz část 4.5).
>
> V České republice působili v roce 2010 tři kvalifikovaní poskytovatelé certifikačních služeb (tj. takoví, kteří vydávají kvalifikované certifikáty). Všichni tři úspěšně prošli akreditací.[15]

Ve druhém případě je důraz kladen na to, aby zaručený elektronický podpis byl vytvářen či ověřován pomocí „bezpečného prostředku“: **bezpečného prostředku pro vytváření elektronických podpisů,**[16] resp. **bezpečného prostředku pro ověřování elektronických podpisů.**[17]

> O zaručených podpisech, které jsou založeny na kvalifikovaných certifikátech a jsou vytvořeny pomocí prostředku pro bezpečné vytváření elektronických podpisů, se hovoří jako **o kvalifikovaných elektronických podpisech.**[18]

Zajímavé je, že obě varianty – tedy jak uznávaný, tak i kvalifikovaný elektronický podpis – mohou skýtat dostatečně vysokou úroveň důvěryhodnosti, tak aby je bylo možné položit na roveň vlastnoručními podpisu na listinném dokumentu či vyžadovat v „úředním styku“ (při komunikaci s orgány veřejné moci).

---

15 Konkrétně jde o společnosti I.CA, která získala akreditaci 18. března 2002, PostSignum (3. srpna 2005) a eIdentity (27. září 2005)

16 V angličtině: SSCD (Secure Signature Creation Device)

17 V angličtině: SSVD (Secure Signature Verification Device)

18 Samotný termín „kvalifikovaný elektronický podpis“ není přímo pojmem zákona, ten jej definuje pouze opisně (jako zaručený podpis, založený na kvalifikovaném certifikátu a vytvořený prostřednictvím prostředku pro bezpečné vytváření elektronických podpisů).

Různé země ale mohou dávat přednost jedné či druhé variantě, což lze dokumentovat i na příkladu České republiky a Slovenska: zatímco na Slovensku dávají přednost použití bezpečných prostředků (a tím kvalifikovaným elektronickým podpisům), v České republice je v tomto ohledu dávána přednost požadavkům na vydavatele certifikátu (cestou jeho akreditace) – a tím i uznávaným podpisům.

A to i přesto, že konkrétně náš zákon[19] explicitně řeší i bezpečné prostředky pro vytváření a ověřování elektronických podpisů, když na ně klade konkrétní požadavky a jejich použití explicitně přisuzuje určité konkrétní důsledky. Například když ve svém §3 konstatuje, že:

> *Použití zaručeného elektronického podpisu, založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu, umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.*

Tomu ale není možné rozumět v tom smyslu, že takovéto ověření umožňuje „až" (či „pouze") použití bezpečného prostředku. Umožňuje ho i uznávaný elektronický podpis, a to díky „kvalitě" své vazby mezi certifikátem a podepsanou osobou. Jen to o něm není takto explicitně konstatováno v zákoně – ale vyplývá to z jeho vlastností a konkrétně i z požadavků na vydavatele certifikátů, které jsou zakotveny v dalších předpisech a vyhláškách.[20]

Fakticky se tak kvalifikované elektronické podpisy a uznávané elektronické podpisy dostávají vzájemně na roveň, i když formálně (ze své definice) to jsou různé druhy elektronických podpisů.

4.4.1 Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

Když už jsme zmínili bezpečné prostředky pro vytváření a ověřování elektronických podpisů, zastavme se ještě na chvíli u toho, jak jsou vnímány zákonem, ale i dalšími právními předpisy, včetně evropských doporučení a směrnic či tuzemských vyhlášek: z nich v zásadě vyplývá, že takovéto „bezpečné prostředky" již nemohou být čistě softwarovými nástroji, ale musí to být hardwarová zařízení (a jen s nějakým „pevně zadrátovaným" firmwarem).

> Konkrétním příkladem bezpečného prostředku může být čipová karta Starcos 3.0, kterou svým zákazníkům v ČR distribuuje I. CA. Ministerstvo vnitra ČR ji v červenci 2010 certifikovalo[21] jako prostředek pro bezpečné vytváření elektronických podpisů, a to jako první v ČR.

---

19 Zákon č. 227/2000 Sb., o elektronickém podpisu.

20 Mj. ve vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

21 „Vyslovilo shodu nástroje elektronického podpisu v souladu se zákonem 227/2000 Sb. o elektronickém podpisu".

4.5 Uznávaný elektronický podpis

V České republice se tedy v běžné praxi „úředního styku“ setkáme s tou variantou zaručeného podpisu, která je založena na použití kvalifikovaného certifikátu – a ten musí být vydán takovým poskytovatelem certifikačních služeb, který je na tuto svou činnost akreditován.

Jelikož by ale vymezení takovéhoto podpisu stylem:

> *zaručený elektronický podpis, založený na kvalifikovaném certifikátu, vydaném akreditovaným poskytovatelem certifikačních služeb …*

bylo příliš dlouhé, byla pro něj zavedena již výše naznačená „zkratka“, a to **uznávaný elektronický podpis.** Neformálně si to lze vyložit (a podle toho i pamatovat) tak, že jiný elektronický podpis orgány veřejné moci (tedy například úřady) neuznávají. Ani nemohou, protože tak jim to přikazuje zákon[22] ve svém §11/1, který současně zavádí samotný pojem „uznávaného podpisu“:

> *V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis“). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.*

Samozřejmě to má svou logiku: pokud něco od státu (či samosprávy) požadujeme, příslušný orgán chce mít (dostatečnou) jistotu ohledně toho, kdo mu požadavek posílá. Proto vyžaduje kvalifikovaný certifikát a požaduje, aby tento certifikát byl vystaven akreditovanou certifikační autoritou. Tedy takovou, jejíž důvěryhodnost a způsob fungování si stát sám prakticky ověřil, v rámci procesu udělování akreditace.

Pokud by stát požadoval pouze zaručený elektronický podpis, ale nikoli již uznávaný, měl by prakticky záruku jen o neporušené integritě (tj. že s obsahem podání nebylo nějak manipulováno). Neměl by ale dostatečnou jistotu ohledně toho, kdo mu podání podává. Viz výše uvedený příklad se zaručeným elektronickým podpisem literární postavy Josefa Švejka.

Po technické stránce (co do způsobu svého vzniku a ověřování) je ale uznávaný podpis úplně stejný jako zaručený elektronický podpis: vzniká postupy a technikami asymetrické kryptografie, pomocí stejných prostředků (ne nutně certifikovaných jako „bezpečné“), s využitím soukromého klíče, a je vyhodnocován pomocí veřejného klíče. Rozdíl je skutečně pouze v požadavcích na certifikát, na kterém je podpis založen.

4.5.1 Jak se pozná uznávaný elektronický podpis?

Zajímavou a pro praxi velmi důležitou otázkou je také to, jak se na konkrétním elektronickém podpisu pozná, zda je pouze zaručený, nebo již uznávaný?

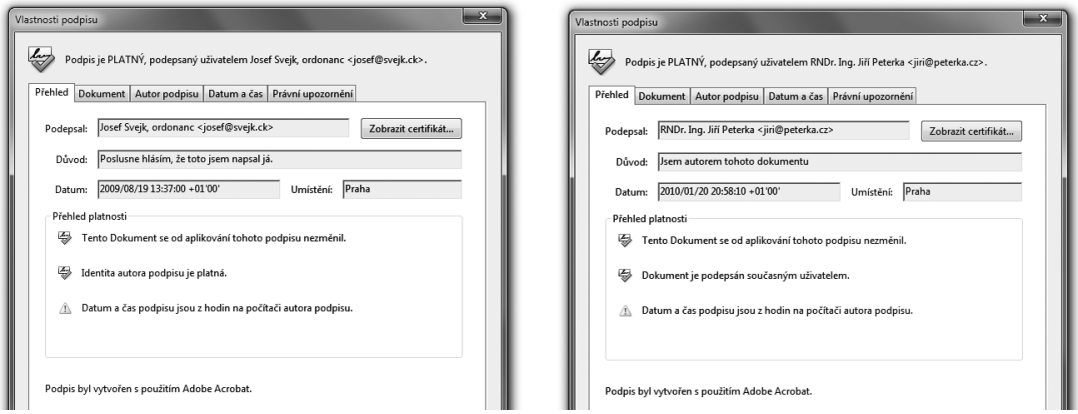
---

22 Zákon č. 227/2000 Sb. o elektronickém podpisu, v platném znění.

To bohužel není tak jednoduché a na první pohled se to vlastně nepozná vůbec. Přesněji: programy, které používáme k vyhodnocování platnosti elektronických podpisů, nám to samy od sebe neřeknou. Schválně, zkuste to zjistit z následujícího obrázku, který ukazuje výsledky vyhodnocení dvou různých elektronických podpisů programem Adobe Reader: ten vlevo patří literární postavě Josefa Švejka a je pouze zaručený, nikoli ale uznávaný. Ten vpravo je podpisem autora tohoto textu a je uznávaný.

Obrázek 4-10

Srovnání zaručeného el. podpisu (vlevo) a uznávaného el. podpisu (vpravo), tak jak je vyhodnocuje program Adobe Reader



To, že z výsledného verdiktu nepoznáme, o jaký druh elektronického podpisu se jedná, má nesmírně závažnou příčinu: běžné prostředky (programy), které používáme pro vyhodnocování zaručených elektronických podpisů (jako Adobe Reader či programy z MS Office) mají jednodušší pohled na celou hierarchii elektronických podpisů.

Programy (prostředky) pro vyhodnocování elektronických podpisů obvykle nerozlišují různé druhy elektronických podpisů. Neznají tedy například rozdíl mezi zaručeným a uznávaným elektronickým podpisem.

Vysvětlení této disproporce je nejspíše takové, že tyto programy pro vyhodnocování (zaručených) elektronických podpisů jsou vyvíjeny jako univerzální, tak aby je bylo možné nasadit v různých zemích s různou legislativou, a navíc je nebylo nutné měnit s každou změnou legislativy, která přinese nějakou změnu v oblasti elektronického podpisu. Zřejmě proto se tyto programy nepokouší hodnotit „jemné právní nuance“, spojené s mírou důvěryhodnosti certifikátu v dané zemi. Místo toho pracují jen s jednoduchou dichotomií: certifikát pro ně buďto je důvěryhodný (pokud je uložen v jejich úložišti důvěryhodných certifikátů), nebo „se neví“ (nemají dostatek informací o jeho důvěryhodnosti).[23] Z toho pak ale nepoznají, o jaký druh podpisu jde.

[23] V některých specifických případech (konkrétně u systémového úložiště certifikátů v MS Windows) mohou mít ještě explicitní informaci o tom, že některé konkrétní certifikáty jsou nedůvěryhodné, viz části 1.13 a 5.4.2.3.

Detailní posouzení kvality certifikátu – a tím i hodnocení druhu elektronického podpisu – tak fakticky zůstává až na uživateli: je na něm, aby konkrétní certifikát správně vyhodnotil.

Rozdíl mezi uznávaným a (pouze) zaručeným podpisem musíme rozpoznat sami, podle druhu certifikátu, na kterém je podpis založen – viz část 4.3.6.

4.5.2 Platnost elektronického podpisu z pohledu programů

V důsledku předchozího odstavce si musíme znovu poupravit naši představu o tom, jak přesně se v praxi vyhodnocuje platnost elektronického podpisu, pomocí běžně používaných prostředků pro ověřování (vyhodnocování platnosti) elektronických podpisů.

Postup, který jsme si popisovali v celé předchozí kapitole, nebral do úvahy druh certifikátu, resp. jeho „kvalitu“ (chápanou jako míru jeho důvěryhodnosti). Zejména tedy to, zda jde o certifikát kvalifikovaný, nebo komerční.

> To odpovídá pohledu (tuzemské) právní úpravy: podle ní druh certifikátu nerozhoduje o platnosti elektronického podpisu: podpis je platný bez ohledu na druh certifikátu, na kterém je podpis založen. Druh certifikátu rozhoduje pouze o tom, zda jde o zaručený elektronický podpis, či o uznávaný elektronický podpis atd.

Běžně používané programy (prostředky) pro vyhodnocování elektronických podpisů ale vyžadují splnění jedné další podmínky, aby konkrétní podpis vyhodnotily jako platný: musí mít explicitní důvod, na základě kterého mohou považovat za důvěryhodný ten certifikát, na kterém je posuzovaný podpis založen.

V praxi to znamená, že buďto musí být označen jako důvěryhodný (vložen do příslušného úložiště důvěryhodných certifikátů) přímo ten certifikát, na kterém je ověřovaný podpis založen, nebo musí být jako důvěryhodný označen některý z jeho nadřazených certifikátů (na příslušné certifikační cestě).

> Názorně to ukazuje předchozí příklad s elektronickým podpisem literární postavy Josefa Švejka (v levé části obrázku 4.10): vyhodnocení platnosti prováděl program Adobe Reader, přičemž certifikát Josefa Švejka byl v jeho úložišti uložen mezi důvěryhodnými certifikáty. Proto jej Reader považoval za důvěryhodný a mohl dospět k závěru, že podpis, založený na tomto certifikátu, je platný.

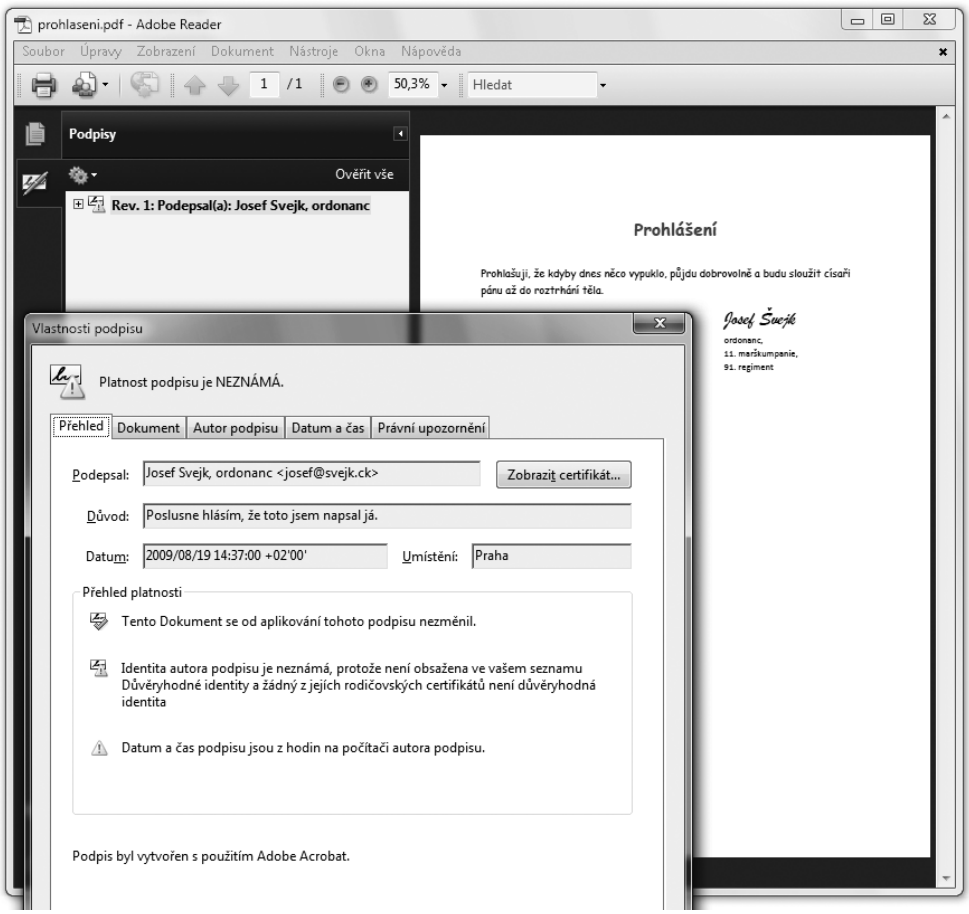
Naopak v případě, kdy ověřující program (prostředek) nemá k dispozici takové informace, na základě kterých by příslušný certifikát (nebo některý z jeho nadřazených certifikátů) mohl považovat za důvěryhodný, nemůže dojít k závěru, že podpis je platný. A to ani tehdy, když jsou ostatní podmínky splněny (tj. integrita podepsaného dokumentu je neporušena, certifikát je platný a nebyl revokován). V takovém případě skončí ověřování podpisu obvykle s výsledkem „nevím“ (i když podle zákona by mělo skončit verdiktem „platný“).

> Příklad ukazuje následující obrázek se stejným zaručeným elektronickým podpisem literární postavy Josefa Švejka jako dříve (v levé části obrázku 4.10). Tentokráte ale bez toho, že by příslušný certifikát byl uložen v tom úložišti důvěryhodných certifikátů, které právě používá program Adobe Reader. Ten tak nemá k dispozici informace, na jejichž základě by certifikát mohl považovat za důvěryhodný – a proto celý podpis hodnotí tak, že jeho platnost je neznámá.

V obou příkladech (na obrázku 4.11 a v levé části obrázku 4.10) přitom jde o jeden a tentýž podpis, který z pohledu práva je platným zaručeným elektronickým podpisem, ale není platným uznávaným elektronickým podpisem.

Obrázek 4-11

Vyhodnocení platnosti podpisu literární postavy Josefa Švejka v situaci, kdy jeho certifikát není zařazen mezi důvěryhodnými certifikáty



Právě popsané chování programů, používaných pro ověřování elektronických podpisů, má velmi významné důsledky pro běžnou praxi: jako uživatelé těchto programů si musíme dávat bedlivý pozor na správnou interpretaci jejich verdiktů. Když nám tyto programy řeknou, že konkrétní podpis je platný, musíme si sami zjistit, zda jde o platný zaručený podpis, platný uznávaný podpis či jiný druh podpisu. A když nám naopak řeknou, že platnost podpisu nedokáží ověřit (tj. že platnost podpisu je neznámá), může to být způsobeno jen tím, že příslušný certifikát není umístěn *na správném místě v úložišti důvěryhodných certifikátů*.

Uvědomme si také, že pokud tyto důležité skutečnosti nebudeme brát v úvahu, bude to jen a jen naše chyba: budeme-li verdikt programu interpretovat chybně a budeme-li podle toho jednat, poneseme případné následky také jen my.

4.5.3 TSL, Trusted Services List

Připomeňme si ještě, že k tomu, aby konkrétní (zaručený) elektronický podpis byl uznávaným elektronickým podpisem, musí být splněny dvě podmínky. Obě se týkají certifikátu, na kterém je podpis založen, a obě musí být splněny současně:

- certifikát musí být kvalifikovaný
- certifikát musel vydat akreditovaný poskytovatel certifikačních služeb

Jak se ověřuje splnění první podmínky jsme si ukazovali v části 4.3.6: kvalifikované certifikáty, vydané tuzemskými certifikačními autoritami, to mají v sobě explicitně napsáno. Takže je třeba se podívat dovnitř certifikátu, na správné místo: buďto přes „Prohlášení vystavitele“, nebo přímo do položky „Zásady certifikátu“.

Splnění druhé podmínky se dříve dalo ověřit také relativně jednoduše: zákon pamatoval jen na tuzemské poskytovatele certifikačních služeb s akreditací, a ti jsou (k roku 2010) pouze tři: společnosti I.CA, PostSignum a eIdentity.[24]

Jenže novela zákona o elektronickém podpisu[25] v březnu 2010 rozšířila již citované vymezení uznávaného elektronického podpisu tak, aby pro něj mohly být využity i certifikáty zahraničních certifikačních autorit, akreditované (nebo tzv. dohledované) v Evropské unii.

---

[24] Nezapomínejme ale na to, že tyto certifikační autority (poskytovatelé certifikačních služeb) nevydávají jen kvalifikované certifikáty, ale také další druhy certifikátů. Takže rozhodně neplatí to, že by jakýkoli certifikát, vydaný takovouto certifikační autoritou, byl automaticky kvalifikovaný.

[25] Konkrétně zákon č. 101/2010 Sb.

Nejprve si připomeňme původní vymezení uznávaného podpisu:[26]

> *V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.*

K tomu bylo nově přidáno ještě toto rozšíření:

> *Za elektronický podpis splňující požadavky odstavce 1 se považuje rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled.*

Tuto poměrně složitou formulaci si můžeme přeložit do běžné češtiny tak, že jde vlastně o to samé jako v tuzemsku, jen s „prodloužením" do EU. Aby mohl být zaručený elektronický podpis, založený na zahraničním certifikátu, hodnocen jako uznávaný, musí být splněny podmínky, týkající se:

- druhu certifikátu (musí to být *„kvalifikovaný certifikát vydaný v rámci služby vedené v seznamu důvěryhodných certifikačních služeb"*)
- vydavatele certifikátu (musí být akreditován, nebo je nad jeho činností vykonáván dohled)

Jak je vidět, jde o obdobné podmínky jako „v tuzemsku". Mírně odlišná jsou pouze přesná kritéria pro jejich splnění, daná rozdíly v legislativních úpravách elektronického podpisu v členských zemích EU.[27]

K tomu, aby se dalo co nejsnáze posoudit, který poskytovatel certifikačních služeb (která certifikační autorita) splňuje požadovaná kritéria, mají jednotlivé členské země nově povinnost zveřejňovat **seznam důvěryhodných služeb**, zmiňovaný v již citovaném rozšíření definice uznávaného podpisu.

Anglicky se tento seznam jmenuje **Trusted Services List**, zkratkou **TSL**, a každá členská země má povinnost vydávat svou národní verzi tohoto seznamu, popisující její „národní" poskytovatele. Za Českou republiku tento seznam najdete na adrese *http://TSL.gov.cz*.

Nad jednotlivými „národními seznamy" TSL pak existuje zastřešující rozcestník, odkazující na jednotlivé národní seznamy. Tento rozcestník spravuje přímo EU, a k jeho obsahu se lze nejsnáze dostat přes stejnou adresu, jako k českému TSL (tj. přes adresu *http://TSL.gov.cz*).

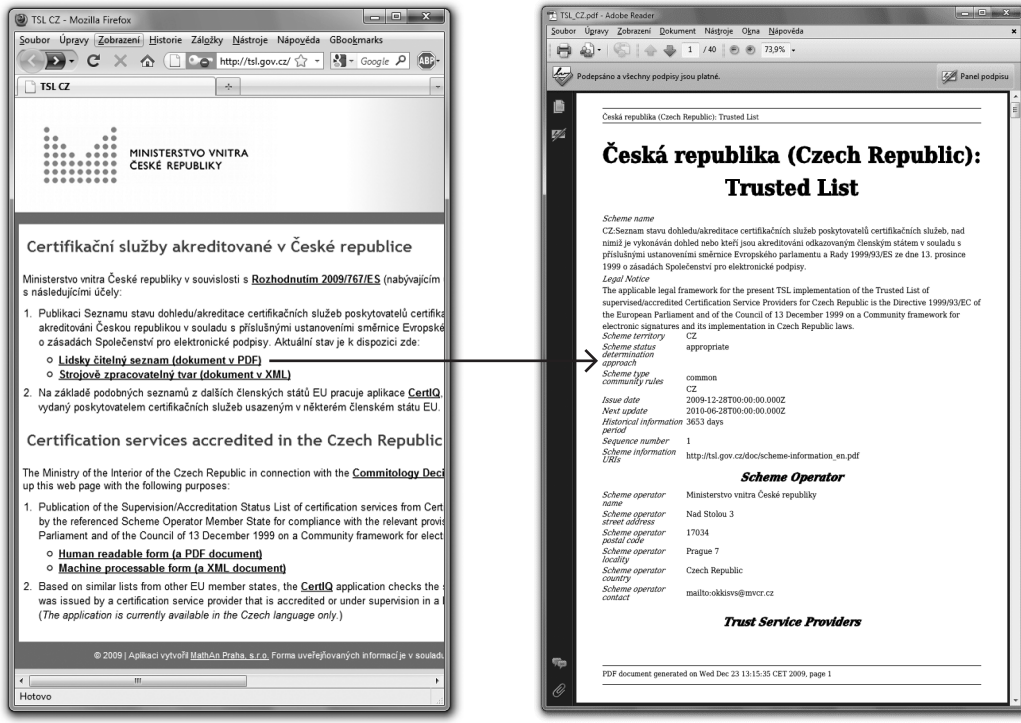
---

[26] §11, odstavec 1 zákona č. 227/2000 Sb., o elektronickém podpisu.

[27] Rozdíl je například v tom, že v ČR je kladen důraz na akreditaci poskytovatelů, zatímco v zahraničí postačuje to, že dozorový orgán státu vykonává nad jeho činností dohled.

Obrázek 4-12

Český seznam TSL



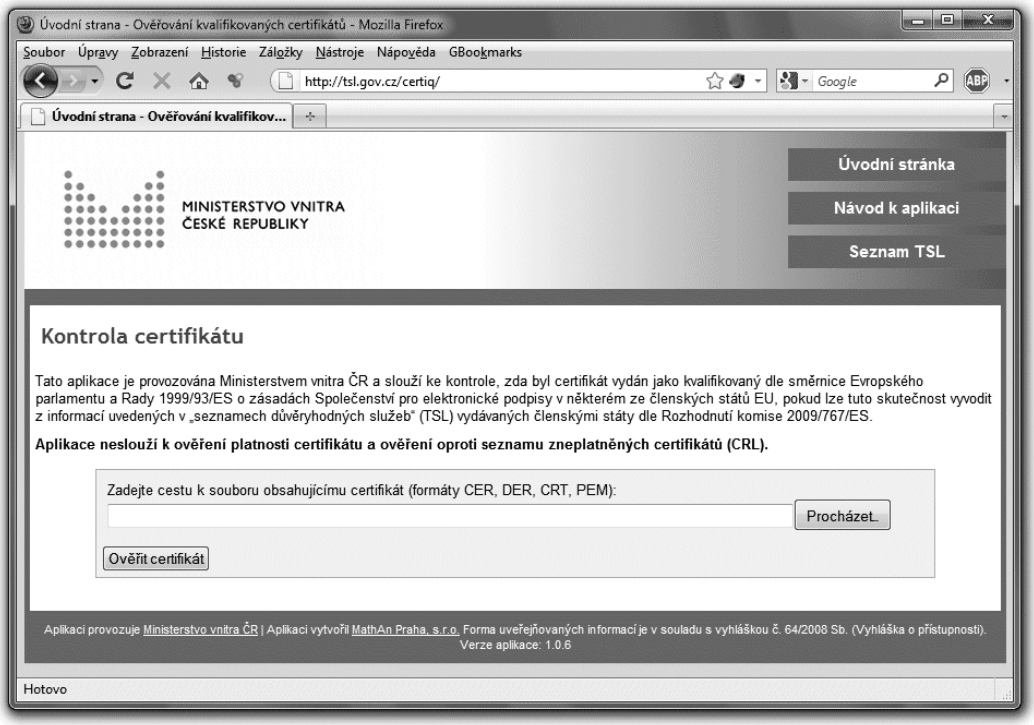
4.5.4 Aplikace CertIQ

Pro hodnocení toho, zda konkrétní elektronický podpis, založený na zahraničním certifikátu, je či není uznávaný, bohužel nestačí podívat se na příslušný národní seznam TSL, zda na něm příslušný vydavatel certifikátu je či není uveden.[28] Stejně jako u certifikátů od tuzemských poskytovatelů musíme vždy ověřit ještě splnění druhé podmínky, kterou je to, zda jde o kvalifikovaný certifikát. Protože stejně jako u nás mohou i zahraniční certifikační autority vydávat různé druhy certifikátů.

Rozpoznat „kvalifikovanost" u tuzemského certifikátu je relativně snadné, jak jsme si již dříve ukazovali: podle naší legislativní úpravy elektronického podpisu to každý kvalifikovaný certifikát musí mít v sobě napsáno. V případě certifikátů od zahraničních vydavatelů to ale může být složitější a obecně je zde třeba vycházet z obsahu příslušné certifikační politiky, podle které byl certifikát vydán. Odkazy na tyto politiky jsou sice na seznamech TSL také uvedeny, ale jejich detailní procházení a správná interpretace je většinou již nad možnosti běžného koncového uživatele.

28 Nestačí dokonce ani to, zda byl vydán v rámci služby, uvedené na seznamu TSL.

Obrázek 4-13
Aplikace CertIQ



Ministerstvo vnitra ČR, ve snaze vyřešit tento problém, nechalo vytvořit on-line aplikaci, které lze předat konkrétní certifikát a která na základě seznamů TSL zjistí, zda je možné ho považovat za kvalifikovaný ve smyslu platných zákonů. Jde o aplikaci jménem CertIQ, kterou lze najít na adrese *http://TSL.gov.cz/certiq/*.Tato aplikace ale skutečně hodnotí pouze to, zda jí předložený certifikát je či není kvalifikovaný. Nehodnotí již další aspekty, konkrétně třeba aktuální platnost certifikátu. Tu si musí ověřit sám uživatel.

Aplikace CertIQ svého uživatele upozorní alespoň na ty skutečnosti, které vyplývají přímo z obsahu samotného certifikátu. Tedy třeba na to, že již skončila řádná platnost certifikátu. Už ale nezkoumá to, zda nedošlo k jeho předčasnému zneplatnění (revokaci).

4.6 Elektronická značka

Připomeňme si, že u elektronického podpisu se předpokládá, že jej vytváří člověk – a že se vždy nejprve seznámí s tím, co podepisuje.[29] To by ale nešlo splnit tam, kde elektronický podpis vytváří nějaký stroj (program) bez přímé účasti člověka. Například u různých výstupů z informačních systémů, které jsou generovány zcela automaticky a v takovém počtu, že by zde přímé zapojení člověka nepřipadalo v úvahu.

Proto byly v roce 2004 do našeho právního řádu zavedeny **elektronické značky**.[30] Vychází vstříc tomu, aby člověk již nemusel asistovat u každého jednotlivého podpisu (vlastně už značky). Místo toho se u značek počítá s tím, že člověk jednorázově nastaví stroj (program) tak, jak je třeba – a ten pak již generuje jednotlivé značky sám, bez přímé lidské účasti.

Zavedení elektronických značek si ale vynutilo několik dalších změn. Počínaje změnami v terminologii:

- místo o podepisování se u elektronických značek mluví **o označování** (jako generování značek)
- také podepsanou či podepisující osobu u elektronických značek nahrazuje **označující osoba.** Ta ale přímo negeneruje jednotlivé značky (to dělá stroj), ale pouze nastavuje a řídí stroj, který následně značky generuje jednotlivé značky již bez přímé lidské účasti.

Dále se muselo upustit od předpokladu, který platí u elektronického podpisu: že podepisující osoba se seznámila s tím, co podepisuje. To u elektronických značek není možné již z ryze praktických důvodů (člověk by to nestíhal), ale někdy i z principiálních důvodů: například u datových zpráv, které prochází skrze datové schránky, se člověk (například zaměstnanec provozovatele či správce) ze zákona ani nesmí seznámit s jejich obsahem. V případě elektronických značek se tedy nepředpokládá, že by se označující osoba seznámila s obsahem toho, co je označováno.

Snad největší změna se ale týká certifikátů a toho, komu mohou být vystaveny (a tím i kdo může být označující osobou). Zatímco u elektronických podpisů se používají osobní certifikáty, vystavované pouze fyzickým osobám (a elektronický podpis tudíž může patřit jen fyzické osobě), elektronické značky musí být založeny na systémových certifikátech (podrobněji popisovaných v části 4.3.3). A ty již mohou být vystaveny jak fyzické osobě, tak i právnické osobě či dalším obdobným subjektům (například organizační složce státu).

Jinými slovy: elektronická značka, na rozdíl od elektronického podpisu, již může „patřit" i právnické osobě.

---

29 Tento předpoklad vychází z obsahu §3 odst. 1 zákona č. 227/2000 Sb.: „*Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila*".

30 Novelou zákona č. 227/2000 Sb., konkrétně zákonem č. 440/2004 Sb.

Obrázek 4-14

Příklad elektronické značky na datové zprávě, přijaté do datové schránky

Po technické stránce je ale elektronická značka shodná se zaručeným elektronickým podpisem.

Ostatně, i zákon definuje elektronickou značku velmi podobně jako zaručený elektronický podpis (viz část 4.2), konkrétně jako:

> *údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky:*

- *jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,*
- *byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,*
- *jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat*

Nepříliš významný rozdíl oproti definici zaručeného podpisu je v tom, že došlo ke sloučení prvních dvou odrážek (u podpisu) do jedné (u značky). Další rozdíly pak jsou dány změnou terminologie (označující vs. podepsaná osoba).

4.6.1 Uznávaná elektronická značka

Podstatnějším rozdílem mezi zaručeným podpisem a elektronickou značkou je ale zmínka o kvalifikovaném certifikátu: definice zaručeného elektronického podpisu žádnou zmínku o „kvalitě“ certifikátu ještě neobsahuje (když hovoří pouze o možnosti identifikace podepsané osoby ve vztahu ke zprávě), a tudíž nutně nevyžaduje ani kvalifikovaný certifikát. Proto jsme si také v předchozím textu mohli ukázat zaručený elektronický podpis literární postavy Josefa Švejka.

Definice elektronické značky už ale kvalifikovaný certifikát zmiňuje (když hovoří o tom, že identifikace označující osoby má být možná skrze použitý kvalifikovaný systémový certifikát).

Elektronická značka je tedy přeci jen „silnější“ než zaručený podpis. Správně, podle její „právní síly“, bychom ji měli klást na roveň zaručenému elektronickému podpisu, založenému na kvalifikovaném certifikátu.

V naší legislativě ale existuje i pojem **uznávaná elektronická značka**. Objevuje se v zákoně č. 300/2008 Sb. (o elektronických úkonech a autorizované konverzi dokumentů), konkrétně v jeho §20, když říká, že datová zpráva má být opatřena elektronickou značkou, založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaná elektronická značka“).

Fakticky se tedy uznávaná elektronická značka liší od elektronické značky (bez přívlastku) v požadavku na to, aby kvalifikovaný systémový certifikát byl vydán některým akreditovaným poskytovatelem certifikačních služeb, a nikoli jen kvalifikovaným poskytovatelem.

4.6.2 Elektronické značky a systémové certifikáty

Zavedení elektronických značek do legislativy ČR v roce 2004 bylo docela průkopnickým činem a lze konstatovat, že ještě v roce 2010 (kdy vznikal tento text) šlo po právní stránce o řešení unikátní, které jiné země (ve srovnatelné podobě) neměly.[31]

S tím souvisí i to, že vzájemné uznávání kvalifikovaných certifikátů od akreditovaných (či jen dohledovaných) poskytovatelů v EU, popisované výše, se týká pouze osobních certifikátů, a tím jen uznávaných elektronických podpisů – a nikoli systémových certifikátů a na nich založených elektronických značek. Současně to pak znamená, že v ČR lze klást faktické rovnítko mezi elektronické značky a uznávané elektronické značky. Ty první sice vyžadují „jen“ kvalifikované systémové certifikáty, zatímco ty druhé trvají na kvalifikovaných systémových certifikátech od akreditovaných poskytovatelů certifikačních služeb. Ale v ČR jsou všechny certifikační autority (poskytovatelé), vydávající kvalifikované systémové certifikáty, současně i akreditované.[32]

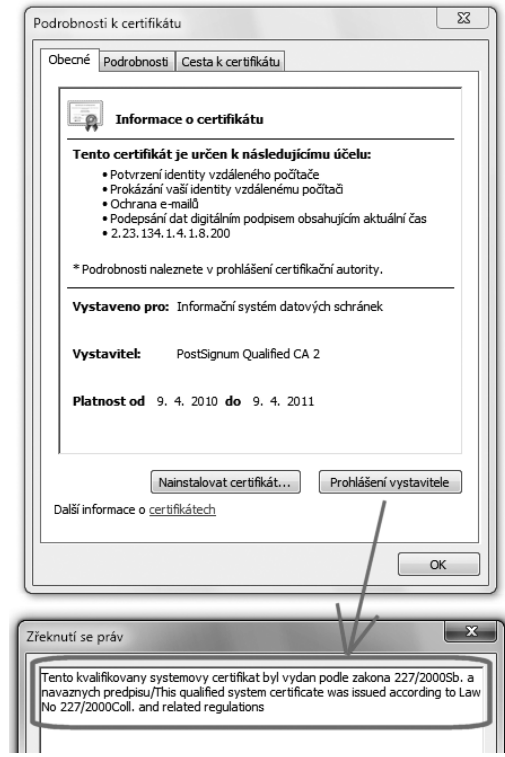
---

[31] Je tomu tak zřejmě proto, že systémové certifikáty „neznají“ příslušné evropské směrnice, a tudíž ani nenařizují jejich podporu.

[32] Pochopitelně ale nelze vyloučit, že v ČR začne v budoucnu působit nějaký další kvalifikovaný poskytovatel certifikačních služeb, který vůbec nepožádá akreditaci.

Omezení jen na „tuzemské“ systémové certifikáty pak značně zjednodušuje i jejich rozpoznání. Stejně jako pro kvalifikované (osobní) certifikáty pro ně totiž platí to, že musí mít v sobě explicitně napsáno, že jsou kvalifikované. Takže stačí podívat se do položky „zásady certifikátu“, buď přímo, nebo přes „Prohlášení vystavitele“, viz obrázek.

Obrázek 4-15
I kvalifikovaný systémový certifikát má v sobě napsáno, že je kvalifikovaný

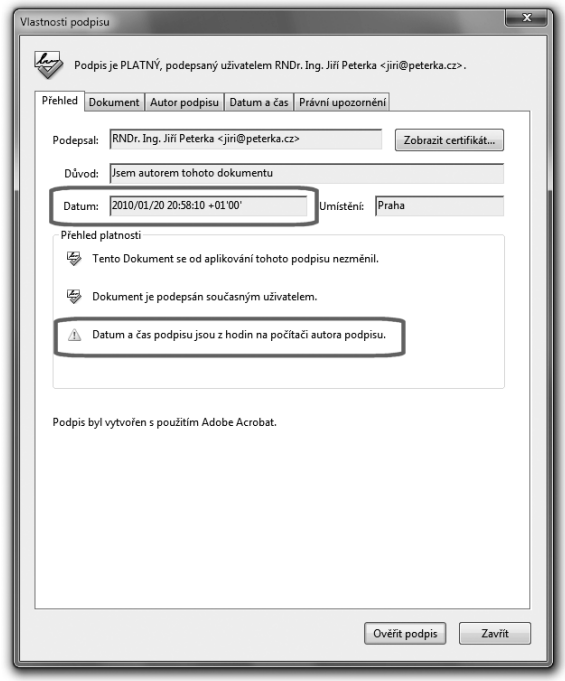


4.7 Časové razítko

Spolu s elektronickými značkami se v roce 2004 dostal do naší národní legislativy další konstrukt, úzce související s elektronickými podpisy: **časové razítko.**

Jeho věcnou podstatu, včetně způsobu vzniku časového razítka, jsme si podrobněji popisovali v kapitole 2, v části 2.7. Proto si jen stručně připomeňme, že časový údaj o době vzniku je sice součástí každého elektronického podpisu, ale jelikož se bere ze systémových hodin na místním počítači, nelze se na tento údaj spoléhat (protože systémové hodiny si uživatel může nastavit tak, jak chce).

Obrázek 4-16
Příklad upozornění na to, že datum a čas podpisu nemusejí být důvěryhodné



Řešením je proto podpis nějaké důvěryhodné třetí strany, která bude ručit za to, že ve svém podpisu uvede správný údaj o čase. Jen se zde místo o podpisu hovoří o časovém razítku.

Připomeňme si také, že časové razítko vzniká tak, že držitel dokumentu z dokumentu nejprve vytvoří otisk (hash), a teprve ten pošle příslušné certifikační autoritě (poskytovateli služby časových razítek). Ta otisk podepíše, s uvedením přesného času kdy se tak stalo – a výsledek (jako časové razítko) vrátí žadateli.

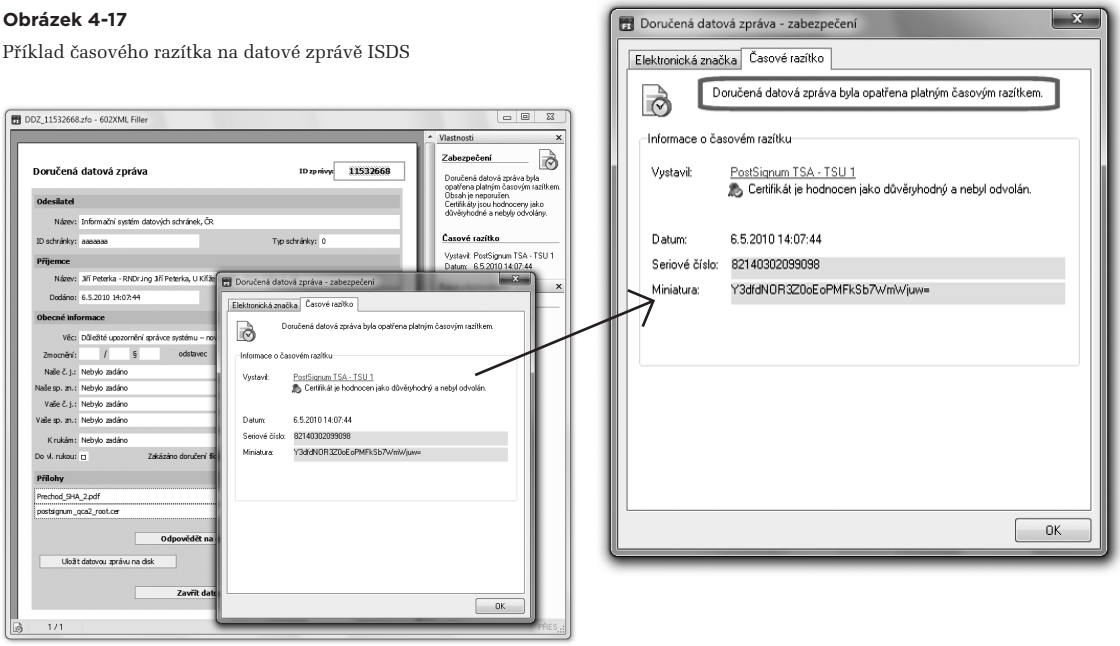
Po právní stránce ale časové razítko skutečně musí být „něco jiného“, než elektronický podpis či elektronická značka. Oba tyto konstrukty (tj. podpis i značka) totiž vyjadřují určitý vztah podepisující osoby k tomu, co je podpisem (značkou) opatřeno, ve smyslu souhlasu, resp. schválení.

V případě časového razítka je tomu ale jinak: vytvoření časového razítka nevyjadřuje vztah charakteru autorství či souhlasu s obsahem, který je časovým razítkem opatřen.

Tím, že poskytovatel přidává na elektronický dokument své časové razítko, nevyjadřuje ani svůj souhlas s tímto obsahem, ale ani svůj nesouhlas. Natož aby pak za tento obsah nějak ručil, byl za něj odpovědný apod.

Obrázek 4-17

Příklad časového razítka na datové zprávě ISDS



Poskytovatel časového razítka nemůže nést odpovědnost za obsah podepsaného dokumentu proto, že nejde o „jeho“ dokument. On k jeho obsahu nezaujímá žádné stanovisko. Podobně jako třeba notář, když ověřuje vlastnoruční podpis na nějakém listinném dokumentu: také pouze ověřuje, kdo dokument podepsal, ale už se nevyjadřuje k tomu, co je podepsáno (k obsahu samotného dokumentu).

Nicméně u časového razítka je ještě jeden významný důvod, kvůli kterému poskytovatel služby časového razítka nemůže zaujmout jakékoli stanovisko k předmětnému dokumentu, i kdyby snad chtěl. Nemá totiž možnost seznámit se s ním. Své časové razítko totiž generuje jen na základě otisku dokumentu, a nikoli celého dokumentu jako takového.

Připojením svého časového razítka tak poskytovatel vyjadřuje a stvrzuje pouze jednu jedinou věc: že to, na co své razítko dává, už v okamžiku přidávání razítka existovalo. A tudíž muselo vzniknout (a tím i existovat) někdy dříve.

Ostatně, ocitujme si ze zákona definici časového razítka:

> *Kvalifikovaným časovým razítkem [se rozumí] datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.*

Povšimněme si, že časové razítko skutečně neříká, jak dlouho „před daným časovým okamžikem“ již existovalo to, co je časovým razítkem opatřeno. Zda to byl nějaký zlomek sekundy, několik hodin či třeba několik let. Ale ono to ani nemusí být podstatné: důležité je, že to existovalo v okamžiku, který je uveden na časovém razítku. A za příslušný časový údaj poskytovatel ručí.

4.7.1 Kvalifikované časové razítko

Na definici časového razítka si povšimněme, že zákon zde vlastně pracuje jakoby až s „vyšším stupněm“, neboli s kvalifikovaným časovým razítkem. Samotné časové razítko (bez přívlastku „kvalifikované“) jako pojem nezavádí. Na druhou stranu použití přívlastku „kvalifikované“ u časového razítka koreluje s požadavkem na to, aby razítko poskytoval takový poskytovatel, který je sám kvalifikovaný.

Jak jsme si již popisovali v části 2.7.1, generování časových razítek probíhá v reálném čase a musí tedy být řešeno strojově. Už jen to vyžaduje, aby samotné časové razítko nebylo svým vydavatelem podepisováno (tj. s přímou účastí člověka), ale opatřováno elektronickou značkou. Což ostatně zákon explicitně požaduje, skrze své požadavky na kvalifikované časové razítko: musí být opatřeno „*elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal*“. A tím pádem (z definice elektronické značky) je jasné i to, že při vydávání časových razítek musí poskytovatel používat kvalifikovaný systémový certifikát.

Na druhou stranu zákon o elektronickém podpisu, ani žádný jiný zákon, nedefinuje ještě vyšší stupeň, a to „uznávané“ časové razítko. Tedy takové, které by kromě požadavku na kvalifikovaný statut poskytovatele ještě vyžadovalo jeho akreditaci (jako je tomu třeba u uznávaných elektronických značek).

> Koncem roku 2010 působili na tuzemském trhu tři kvalifikovaní poskytovatelé služby časových razítek: společnosti I. CA, PostSignum a eIdentity. A všechny tři již měly od státu akreditaci na poskytování služby časových razítek. Takže mezi „kvalifikovaným“ a „uznávaným“ časovým razítkem by nebyl žádný faktický rozdíl.

4.8 Hierarchie podpisů, značek a razítek

Z předchozích odstavců vyplývá, že v ČR existuje a používá se hned několik variant, či spíše „úrovní“ elektronického podpisu, lišících se (z pohledu zákona) svým postavením, významem a důsledky. Tedy jakousi pomyslnou „silou“. Při maximálně detailním pohledu bychom mohli rozlišit až čtyři varianty elektronických podpisů, viz následující tabulka:

„síla“	**varianta elektronického podpisu**
nejvyšší	uznávaný elektronický podpis
	zaručený elektronický podpis, založený na kvalifikovaném certifikátu
	zaručený elektronický podpis
nejnižší	elektronický podpis (bez přívlastku)

V praxi přitom dvě nejvyšší úrovně dlouho splývaly, díky tomu, že všichni tuzemští poskytovatelé, vydávající kvalifikované certifikáty, mají akreditaci od státu. Vzhledem k rozšíření o evropské certifikáty díky seznamům TSL, je ale na místě je (možná jen formálně) stále rozlišovat.[33]

Pro srovnání si připomeňme, že u „papírových" podpisů – tedy u podpisů na listinných dokumentech – také existuje obdobná hierarchie, byť jen tříúrovňová:

„síla"	varianta podpisu
nejvyšší	ověřený vlastnoruční podpis
	vlastnoruční podpis
nejnižší	podpis (bez přívlastku)[34]

Pokud bychom měli obě uvedené hierarchie nějak vzájemně srovnat, alespoň pokud jde o právní kritéria (srovnatelnou „sílu" podpisu), pak určitá ekvivalence by existovala mezi vlastnoručním podpisem a uznávaným elektronickým podpisem, viz následující tabulka. Pokud totiž budete chtít komunikovat s úřady (orgány veřejné moci) elektronickou cestou, pak všude tam, kde byste v listinné podobě museli připojit svůj vlastnoruční podpis, bude po vás v elektronické formě požadován podpis tzv. uznávaný.

„síla"	na dokumentu v listinné podobě	na dokumentu v elektronické podobě
nejvyšší	ověřený podpis	
	vlastnoruční podpis	**uznávaný elektronický podpis**
		zaručený elektronický podpis, založený na kvalifikovaném certifikátu
		zaručený elektronický podpis
nejnižší	podpis (bez přívlastku)	elektronický podpis (bez přívlastku)

Stejně tak by mohla existovat určitá ekvivalence mezi elektronickým podpisem (bez přívlastku) a podpisem (také bez přívlastku). Obojí neskýtá žádnou záruku toho, že jej skutečně vytvořila konkrétní osoba, jejíž identitu podpis vyjadřuje – a oba tyto podpisy by tak měly být považovány jen za určitou informaci a nikoli za podpis.

Zajímavé je spíše to, že „ověřený podpis" na listinném dokumentu, vyžadovaný řadou konkrétních agend, nemá ve světě elektronických podpisů formální ekvivalent.[35] A tak úkony v rámci těchto agend, které trvají na ověřeném podpisu (ať již ověřeném notářsky, soudně či úředně), dodnes nelze realizovat elektronicky.[36]

---

33 Naopak zde není uvažován kvalifikovaný elektronický podpis, který není přímo pojmem zákona (viz část 4.4).

34 Příkladem takového podpisu (bez přívlastku) může být třeba jméno a příjmení osoby, napsané na dokumentu strojem či vytvořené otiskem razítka (se jménem), ale nikoli psané vlastní rukou.

35 Alespoň podle převažujícího právního názoru, resp. chování agend, vyžadujících ověřený vlastnoruční podpis. Existují alei takové právní názory a výklady, které již dnes staví uznávaný podpis na roveň úředně ověřenému vlastnoručnímu podpisu.

Pokud jde o elektronické značky, zde jsme si již uvedli, že zákon definuje dvě různé varianty značek:

„síla“	varianta elektronické značky
nejvyšší	uznávaná elektronická značka
nejnižší	elektronická značka

Fakticky je ale tato dvouúrovňová hierarchie ve skutečnosti jednoúrovňová, protože samotná „elektronická značka“ vyžaduje použití kvalifikovaného (systémového) certifikátu, a všichni tuzemští poskytovatelé certifikačních služeb, kteří vydávají kvalifikované systémové certifikáty, jsou akreditovaní.

Formálně bychom ale měli značky srovnávat s podpisy tak, že „uznávaná“ značka je na stejné úrovni jako „uznávaný“ podpis, zatímco značka (bez přívlastku) by měla být na stejné úrovni jako zaručený podpis, založený na kvalifikovaném certifikátu.

„síla“	varianta elektronického podpisu	varianta elektronické značky
nejvyšší	uznávaný elektronický podpis	uznávaná elektronická značka
	zaručený elektronický podpis, založený na kvalifikovaném certifikátu	elektronická značka (bez přívlastku)
	zaručený elektronický podpis	
nejnižší	elektronický podpis (bez přívlastku)	

4.9 Komu patří elektronický podpis?

Zajímavou otázkou kolem elektronických podpisů, která má spíše právní než technický charakter, je otázka toho, komu „patří“ konkrétní elektronický podpis. Neboli: kdo je **podepsanou osobou?**

Vzhledem k tomu, co o tom již víme, bychom se spíše měli ptát: kdo je držitelem certifikátu?

Na první pohled ale tato otázka nepůsobí příliš logicky: v certifikátu jsou přeci obsaženy údaje, identifikující jeho držitele. A pokud je certifikát dostatečně „kvalitní“ a důvěryhodný (například je kvalifikovaný), můžeme se na jeho obsah spolehnout. Protože ten, kdo certifikát vydal, nám ručí za jeho obsah a tím i za identitu toho, komu certifikát vydal.

Podstata problému je ale někde jinde. Není to o tom, že by v dostatečně důvěryhodném certifikátu byla identita jeho držitele (a tím i podepsané osoby) zfalšována. Je to o tom, že tato identita nemusí být v certifikátu vyjádřena v dostatečném rozsahu na to, aby to stačilo pro jednoznačnou a přesnou identi-

[36] O vytvoření elektronického ekvivalentu pro ověřený podpis se snažil předchůdce dnešního zákona č. 300/2008 Sb., ještěz dílny sdružení eStát (jako tzv. zákon o eGovernmentu). Navrhoval zavedení tzv. legalizovaného elektronického podpisu, který by byl elektronickou obdobou ověřeného podpisu.

fikaci konkrétní osoby někým, kdo má k dispozici právě a pouze daný certifikát. V tom smyslu, že údaje v certifikátu mohou „pasovat“ na více osob, a my mezi nimi nedokážeme spolehlivě rozlišit skutečného držitele.

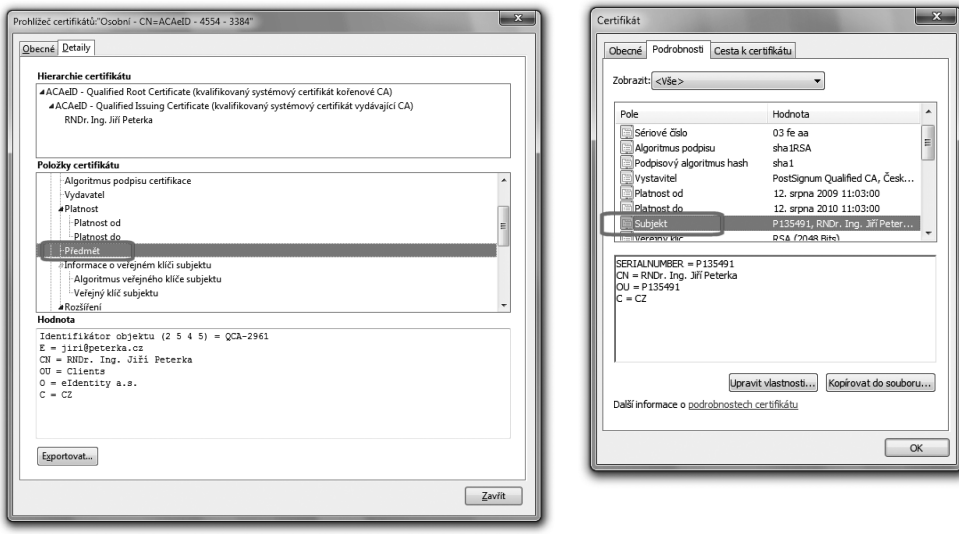
Zákon (č. 227/2000 Sb., o elektronickém podpisu) je totiž v požadavcích na identifikaci držitele certifikátu poměrně minimalistický, když požaduje – a to i od kvalifikovaného certifikátu – jen jméno a příjmení. Místo nich dokonce připouští i pseudonym (viz část 4.9.3), ale naštěstí s povinným upozorněním na to, že jde o pseudonym a nikoli o skutečné jméno či příjmení. Zmiňuje také „zvláštní znaky podepisující osoby“, které musí být v certifikátu obsaženy – ale ty váže jen na případy, kdy to vyžaduje účel certifikátu (jako například u tzv. zaměstnaneckých certifikátů, viz část 4.9.4). V praxi se pak skutečně můžeme setkat i s takovými (kvalifikovanými) certifikáty, které obsahují pouze jméno a příjmení svého držitele, eventuálně i jeho tituly, ale nic víc. Takový certifikát pak může „pasovat“ na mnoho lidí současně, protože i v České republice, s obyvatelstvem v řádu 10 milionů lidí, existují lidé stejného jména a příjmení.

4.9.1 Subjekt certifikátu

V následujících částech si budeme podrobněji popisovat vnitřní strukturu certifikátů. Dozvíme se, že se skládá z více položek, a že jedna z nich samozřejmě identifikuje i držitele certifikátu. Jde o položku, která se v angličtině jmenuje **Subject**, a do češtiny je při zobrazování obsahu certifikátu některými programy překládána jako **Subjekt** (například systémovými utilitami MS Windows), nebo jako **Předmět** (například prohlížečem Mozilla Firefox).

Obrázek 4-18

Prohlížeč Firefox zobrazuje položku „Subject“ jako Předmět, Internet Explorer jako Subjekt



Obsahem položky Subject (Subjekt, Předmět) v rámci certifikátu je řetězec, označovaný jako **Distinguished Name**, zkratkou **DN**. Ten je sám strukturován do několika složek.

V „minimálním případě“ může mít celý řetězec DN jen jednu relevantní složku, která se jmenuje **CN (Common Name)**. V případě fyzické osoby je právě v ní uvedeno jméno a příjmení držitele certifikátu, případně i s tituly. Příklad lze vidět na předchozích dvou obrázcích, které oba ukazují kvalifikované certifikáty. Na druhém z nich tvoří celý řetězec DN čtyři složky:

SERIALNUMBER = P135491
CN = RNDr. Ing. Jiří Peterka
OU = P135491
C = CZ

Řetězec DN (Distinguished Name), popisující držitele certifikátu, ale může obsahovat i další údaje. Dokonce i jakési „sériové číslo“, které je na prvním obrázku uvedeno ve složce „Identifikátor objektu“, a na druhém ve složkách OU (Organizational Unit) a SERIALNUMBER. Nejde přitom o sériové číslo samotného certifikátu, ale o „sériové číslo“ (identifikátor) držitele certifikátu – ovšem jen v rámci interní agendy příslušné certifikační autority, která certifikát vystavila. Tato agenda je ale neveřejná, takže přístup k ní má jen samotná certifikační autorita, a nikoli širší veřejnost.

> Některé certifikační autority (například CA PostSignum) prezentují ve svých certifikačních politikách toto sériové číslo držitele certifikátu jako tzv. rozlišovací jméno, které „jednoznačně identifikuje podepisující resp. označující osobu dle pravidel definovaných příslušnou certifikační politikou“.

Sériové číslo držitele certifikátu může pomoci při „provázání“ dvou různých certifikátů od téhož vydavatele, neboli ke zjištění, zda patří jedné a téže osobě,[37] viz předchozí obrázek.

Běžný uživatel (resp. kdokoli kromě příslušné certifikační autority) už ale nemůže využít toto „sériové číslo“ k bližší identifikaci toho, komu byl certifikát vystaven a kdo je jeho držitelem. Obvykle sice má možnost nechat si vyhledat již vystavené certifikáty i podle tohoto sériového čísla na webu příslušné certifikační autority, ale zde se nedozví o nic víc, než co už je uvedeno na certifikátu. Viz první obrázek na další stránce a jeho srovnání s předchozím obrázkem.

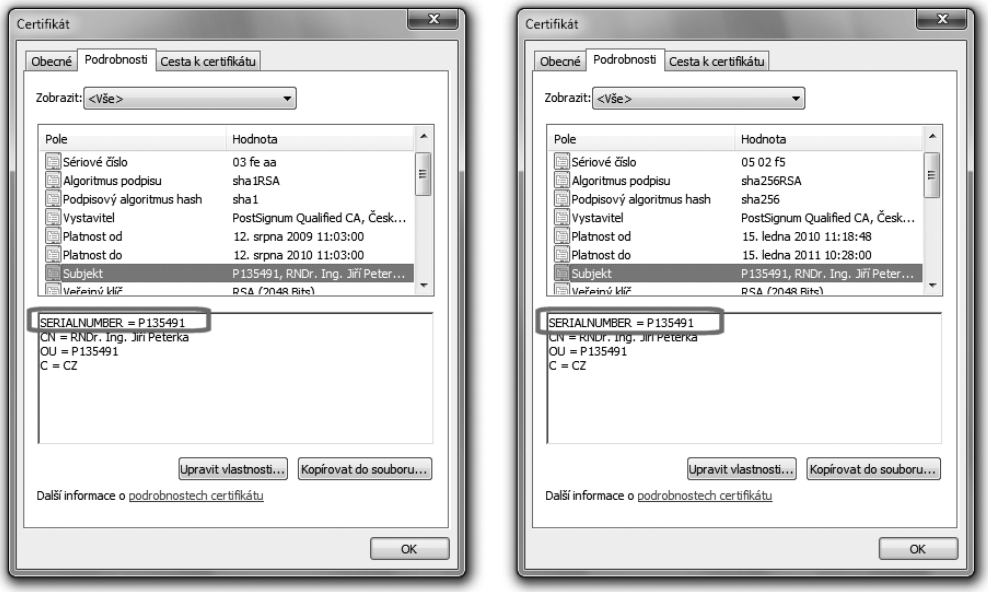
Vlastně: něco navíc se uživatel přeci jen může dozvědět. To, zda certifikát nebyl revokován, neboli předčasně zneplatněn. Toto se totiž ze samotného certifikátu nepozná, a je nutné se na to ptát přímo vydavatele certifikátu, viz část 3.4 a druhý obrázek na následující stránce.

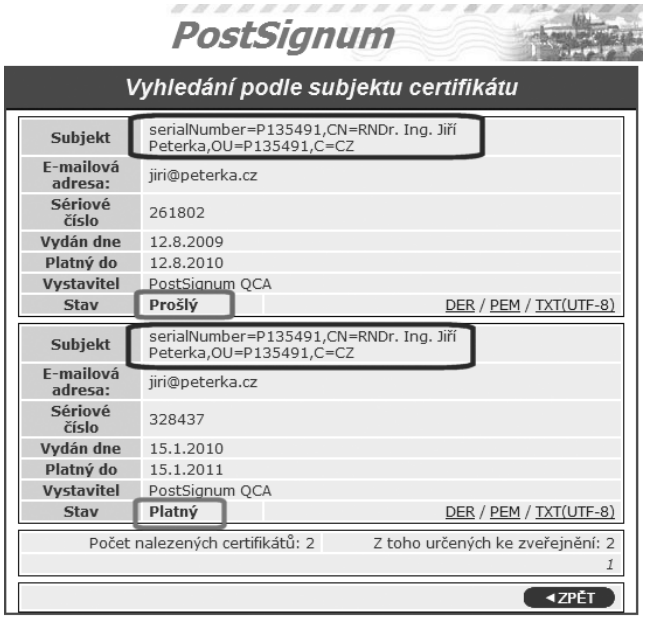
---

[37] Opak ale nutně neplatí: jedna a táž fyzická osoba může být u téže certifikační autority vedena pod různými „sériovými čísly“.

Obrázek 4-19

Dva různé certifikáty, které podle „sériového čísla držitele“ patří stejné fyzické osobě





Obrázek 4-20

Výsledek vyhledání certifikátů podle „sériového čísla“ držitele

4.9.2 Požadavek zákona na jednoznačnou identifikaci držitele certifikátu

Až si budeme popisovat postup při vydávání kvalifikovaného certifikátu (navíc u akreditované certifikační autority), dozvíme se, že ta velmi pečlivě a přesně zjišťuje identitu svého zákazníka, nejméně podle dvou jeho osobních dokladů. Sama tedy velmi přesně ví, o koho jde, a dokáže danou osobu jednoznačně identifikovat.

Problém je ale v tom, že tuto svou „znalost" nemusí přenášet do samotného certifikátu, ani toho kvalifikovaného. Jak jsme si ukázali v předchozích odstavcích, i do kvalifikovaného certifikátu se někdy dostane jen jméno a příjmení, které k jednoznačné identifikaci nepostačují. A pak již jen „sériové číslo" držitele certifikátu (rozlišovací jméno), které jednoznačnou identifikaci umožňuje – ale zase jen tomu, kdo má přístup do interní evidence zákazníků certifikační autority. Což je pouze tato autorita sama.[38]

Celý problém samozřejmě není nový a je určitým způsobem řešen i v zákoně (č. 227/2000 Sb., o elektronickém podpisu). Ten ve svém paragrafu 11 explicitně požaduje, aby certifikát obsahoval takové údaje, aby „osoba byla jednoznačně identifikovatelná".

Ovšem jen v kontextu komunikace s orgány veřejné moci, jen u uznávaného elektronického podpisu a s odkazem na to, že konkrétní požadavky stanoví ministerstvo (vnitra):

> *(§ 11/1) V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen "uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.*

Takovýto prováděcí předpis[39] byl vydán v roce 2004 a stanovil, že:

> *Údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295 a je spravován ústředním orgánem státní správy.*

Číselně tento rozsah přesně odpovídá rozsahu, v jakém je přidělován identifikátor klienta MPSV (Ministerstva práce a sociálních věcí), používaný primárně v rámci systémů tohoto resortu. V praxi je tento identifikátor také skutečně využíván, byť prováděcí předpis explicitně nezmiňuje, že má jít právě o tento identifikátor.

---

38 Případně ještě orgány činné v trestním řízení a další orgány veřejné moci, které k tomu mají zákonné zmocnění.

39 Vyhláška č. 496/2004 Sb. „o elektronických podatelnách".

Možnost blíže identifikovat konkrétní fyzickou osobu podle identifikátoru MPSV (získat další údaje o této osobě, na základě hodnoty identifikátoru) ale mají jen některé orgány státní správy (a také certifikační autority), na základě dohody s MPSV. Ostatní nikoli.

> Například na Slovensku se otázka jednoznačné identifikace řeší vkládáním rodného čísla do certifikátu. V ČR by ale takováto praxe nebyla možná, vzhledem k tomu, že rodné číslo je chráněným osobním údajem, zatímco certifikát je ze své podstaty veřejný.

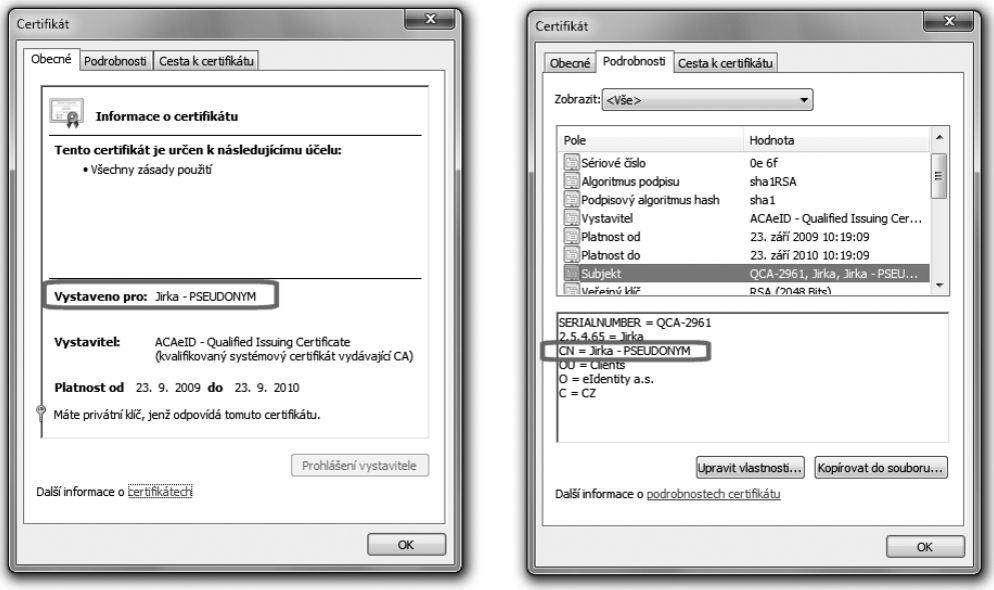
4.9.3 Certifikáty s pseudonymem

Problém s jednoznačnou identifikací držitele certifikátu dále zhoršuje skutečnost, že i kvalifikovaný certifikát může místo jména a příjmení svého držitele obsahovat jen jeho pseudonym (viz požadavky na obsah kvalifikovaného certifikátu v části 4.3.4). Sice s důrazným upozorněním, že jde o pseudonym, ale i tak je to stále jen pseudonym.

U takovéhoto certifikátu se tedy nepozná, komu vlastně patří. A to ani, když si ho necháte vyhledat na webu certifikační autority, která ho vystavila. I zde se dozvíte právě a pouze ty údaje, které jsou již v samotném certifikátu (plus informaci o případné revokaci).

Obrázek 4-21

Příklad certifikátu s pseudonymem



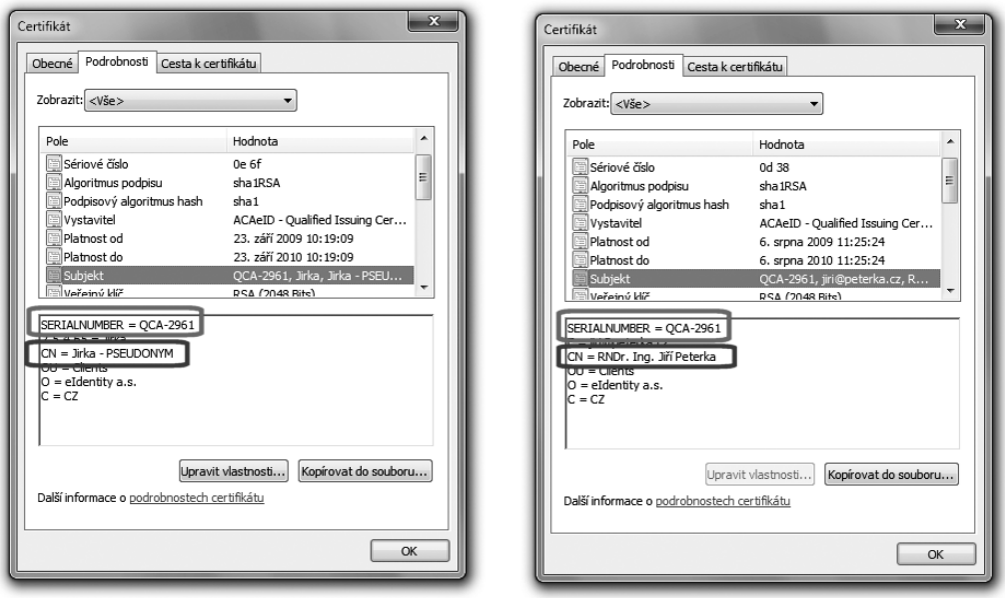
Na druhou stranu i certifikát s pseudonymem může umožňovat jednoznačnou identifikaci svého držitele: certifikační autorita ví naprosto přesně, komu ho vystavila. Běžný uživatel ale nemá moc šancí tuto identitu zjistit.

Nemožnost zjistit, komu certifikát s pseudonymem patří, ale ještě neznamená, že by jeho použití bylo vždy nějak nelegitimní či přímo podvodné. Existuje řada situací, kdy protistrana (například nějaký poskytovatel služby) nepotřebuje znát identitu svého zákazníka. Potřebuje ale zajištěnou „kontinuitu“ mezi jeho jednotlivými požadavky či úkony: budou-li podepisovány s využitím stejného certifikátu (byť s pseudonymem), má protistrana jistotu, že přichází od stejné osoby. I když její identitu nezná.

Někdy je ale přeci jen možné zjistit identitu toho, komu byl certifikát s pseudonymem vystaven. To když certifikační autorita vloží do řetězce DN „sériové číslo“ držitele certifikátu s pseudonymem, a to se shoduje se sériovým číslem na jiném certifikátu, který již je „na jméno“ a nikoli „na pseudonym“. Příklad ukazuje následující obrázek.

Obrázek 4-22

Odhalení pseudonymu prostřednictvím „sériového čísla“ držitele



4.9.4 Zaměstnanecké certifikáty

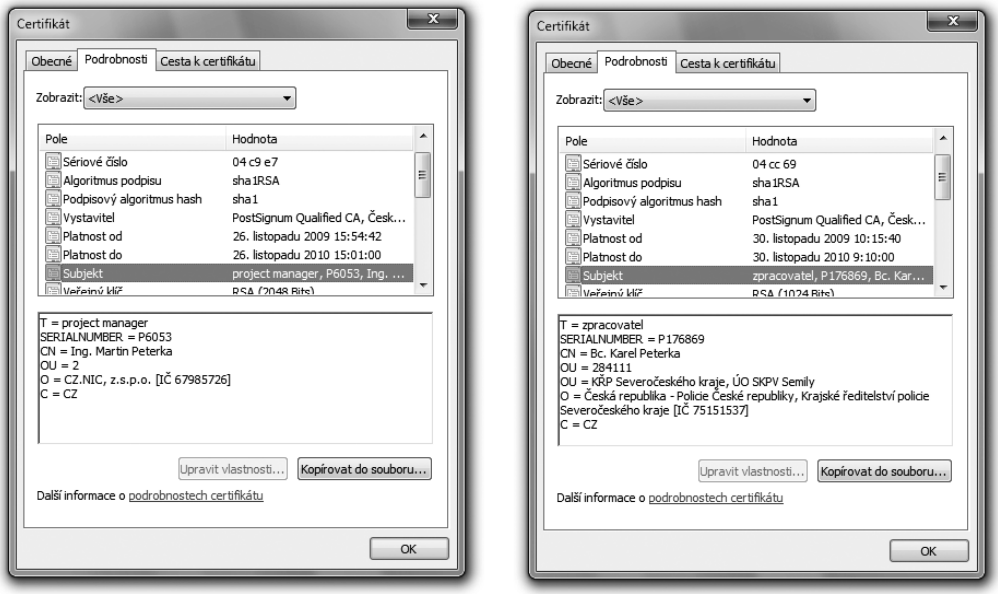
Ještě další variantou osobních certifikátů jsou takové, které kromě identity svého držitele vyjadřují i jeho zaměstnanecký vztah: kdo je zaměstnavatelem držitele certifikátu, případně funkci kterou držitel vykonává, jeho organizační začlenění (kde v rámci organizace zaměstnavatele působí) atd.

Právě kvůli těmto informacím se o těchto certifikátech hovoří jako o „zaměstnaneckých“. Při jejich vydávání musí žadatel prokázat svůj zaměstnanecký poměr. Velmi často jsou také takovéto certifikáty vydávány přímo z iniciativy zaměstnavatele (na jeho objednávku), pro jednotlivé zaměstnance.

Údaj o zaměstnavateli se vkládá přímo do řetězce DN (Distinguished Name), který je obsažen v položce pro držitele certifikátu (Subjekt, případně Předmět). Nejčastěji je údaj o zaměstnavateli obsažen ve složce O (Organization) řetězce DN, případné organizační zařazení je pak vyjádřeno ve složce OU (Organizational Unit) a pracovní zařazení ve složce T (Title). Příklady ukazuje obrázek.

Obrázek 4-23

Příklady zaměstnaneckých certifikátů



Požadavek na to, aby orgány veřejné moci vybavovaly své zaměstnance zaměstnaneckými certifikáty, je obsažen v nařízení vlády z roku 2004.[40] To konkrétně požaduje, aby v rámci zaměstnaneckého certifikátu bylo obsaženo označení orgánu veřejné moci, jeho příslušného organizačního útvaru a zařazení zaměstnance.

40 Nařízení vlády č. 495/2004 Sb., „k provádění zákona o elektronickém podpisu“.

4.10 Platnost elektronického podpisu

Jak jsme si již dříve řekli, problematika posuzování platnosti elektronických podpisů má jak své technické aspekty, tak i své aspekty právní.

Technickým aspektům, které jsou relativně lépe zvládnuté a „zažité“, jsme se věnovali v celé předchozí kapitole, kde jsme se také seznámili s nezbytnými postupy při ověřování platnosti elektronických podpisů či značek.

Proto si jen stručně připomeňme, že toto ověřování může skončit jedním ze tří možných závěrů:

- ano (podpis či značka jsou platné)
- ne (podpis či značka jsou neplatné)
- „nevím“ (není dostatek informací k posouzení platnosti podpisu či značky)

Zapomínat nesmíme ani na faktor času: posuzování platnosti podpisu či značky je vždy vztaženo k určitému časovému okamžiku, ke kterému platnost vyhodnocujeme (k posuzovanému okamžiku).

V praxi je poměrně časté, že k jednomu posuzovanému okamžiku jsem schopni ověřit platnost podpisu či značky (ve smyslu verdiktu „ano“), zatímco k jinému posuzovanému okamžiku nikoli (a musíme skončit verdiktem „nevím“).

Obvykle je to tak, že s plynutím času ztrácíme schopnost ověřit platnost elektronického podpisu či značky: zatímco k nějakému předchozímu posuzovanému okamžiku můžeme při ověřování platnosti dojít k verdiktu „ano“, později už nám třeba nezbývá než konstatovat „nevím“.

> Připomeňme si také, že toto časové omezení je vyvoláváno zcela záměrně, skrze omezenou životnost certifikátů, na kterých jsou elektronické podpisy založeny. Důvodem je potřeba zohlednit vývoj v oblasti kryptografie i růstu výpočetní kapacity počítačů, a včas eliminovat riziko rychlého nalezení kolizních dokumentů, viz část 2.6.

Naproti tomu z pohledu práva podpis neztrácí svou platnost v čase. V celém právním systému není nikde stanoveno, že by podpisy nějak „zastarávaly“ a jejich platnost podpisu byla nějak závislá na čase.[41]

Důležité přitom je, že toto platí pro všechny druhy podpisů, tedy jak pro podpisy vlastnoruční, tak i pro podpisy elektronické. U žádné varianty podpisu není stanoveno, že by platnost podpisu končila v závislosti na čase.

---

[41] Zde je třeba rozlišovat mezi podpisem a úkonem, který je podpisem stvrzen. Podpis nezastarává a nelze ho odvolat. Samotné úkony však mohou mít časově omezené účinky a lze je v některých případech také odvolat (zpětvzetím či novým úkonem apod.).

4.10.1 Platnost podpisu vs. možnost ověřit platnost podpisu

Disproporce mezi časově omezenou možností přesvědčit se o platnosti elektronického podpisu (ověřit tuto platnost) a časově neomezenou platností elektronického podpisu (v právním slova smyslu) nás opravňuje k formulování následující teze:

Platnost elektronického podpisu (značky či razítka) a možnost ověřit tuto platnost jsou dvě různé věci: elektronický podpis nepřestává být platný tím, že přijdeme o možnost pozitivně se přesvědčit o jeho platnosti (tj. ověřit jeho platnost). Stále nám zbývá možnost prokázat jeho platnost nějakým jiným způsobem.

S platností elektronického podpisu je to tedy jako s objektivní realitou, která také existuje nezávisle na tom, zda jsme schopni ji vidět či jinak vnímat, nebo toho nejsme schopni. Když něco nevidíme, ještě to neznamená, že to neexistuje. Takže i když „to" nějakou dobu vidíme, ale pak zavřeme oči (a v důsledku toho přijdeme o možnost vidět), nemůžeme z toho odvozovat, že „to" přestalo existovat.

Představme si to na příkladu sjednání nájemní smlouvy (jako právního úkonu). Tato smlouva ale byla sepsána a podepsána nikoli v listinné podobě, nýbrž v podobě elektronické. V době sepsání byla platnost elektronických podpisů na smlouvě řádně ověřena, smluvní strany považovaly nájem za řádně sjednaný a jednaly podle toho.

Pokud časem (s expirací podpisových certifikátů) přijdeme o možnost ověřit platnost elektronických podpisů na elektronické nájemní smlouvě, mělo by to být důvodem k prohlášení podpisů na této smlouvě za neplatné? A v důsledku toho k prohlášení celé smlouvy za neplatnou a anulování původního právního úkonu? Tedy k vystěhování toho, kdo si nájem sjednal a domníval se, že má kde bydlet?

Určitě nikoli. Pokud by někdo chtěl napadnout již uzavřenou nájemní smlouvu (obecně jakýkoli smluvní dokument) a domáhat se její neplatnosti, musel by tuto neplatnost něčím prokázat. Pokud by to mělo být z důvodu neplatnosti elektronických podpisů na smlouvě, pak by musel prokázat jejich neplatnost. Tedy pozitivně ověřit, že jsou neplatné, resp. že byly neplatné v době svého vzniku. Verdikt ve smyslu „nevím", resp. nemožnost ověřit platnost (či neplatnost) podpisu k tomu stačit nemůže.

Nehledě na to, že protistrana má stále možnost prokázat platnost celé kupní smlouvy jinak. Například listinnou podobou smlouvy, vzniklou autorizovanou konverzí (z elektronické do listinné podoby) ještě v době, kdy bylo možné ověřit platnost podpisů na dokumentu. Nebo nějakou svědeckou výpovědí či ještě jiným způsobem.

4.10.2 Digitální kontinuita

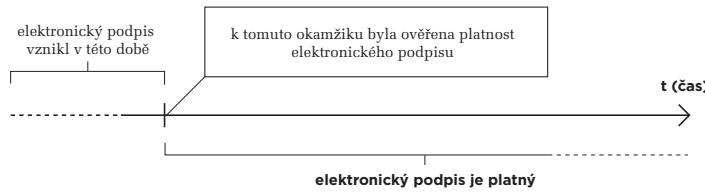
Teze o tom, že platnost elektronického podpisu přetrvává i ztrátu možnosti ověřit si tuto platnost, je samozřejmě velmi podstatná pro dlouhodobou práci s elektronickými dokumenty, i pro možnost uzavírání smluvních vztahů na delší dobu.

> Pokud by tomu tak nebylo a platnost elektronického podpisu by končila s platností certifikátu, na kterém je podpis založen, pak by bylo vše špatně: praktická životnost (použitelnost) elektronických dokumentů by byla omezena nejvýše na 1 rok, stejně jako dopady právních úkonů, činěných elektronickou cestou.

Stejně tak je celá tato teze nesmírně důležitá i z pohledu praxe. Umožňuje nám totiž, abychom ověřili platnost elektronického podpisu k takovému časovému okamžiku, k jakému jsme schopni to provést – a pak se odkázali na tuto tezi a z ní odvodili platnost podpisu i v aktuálním čase (či v jiném čase, který nás zajímá a který následuje po okamžiku, ke kterému se nám podařilo podpis ověřit). Představu, kterou bychom mohli označit jako princip **digitální kontinuity**, ukazuje obrázek.

Obrázek 4-24

Představa digitální kontinuity



Tento princip samozřejmě má jedno důležité omezení: „kontinuita“ může platit jen do té doby, než dojde ke ztrátě platnosti elektronického podpisu z nějakého jiného důvodu.

Z technických důvodů připadá v úvahu zejména porušení integrity v důsledku pozměnění dokumentu, který je podpisem opatřen.

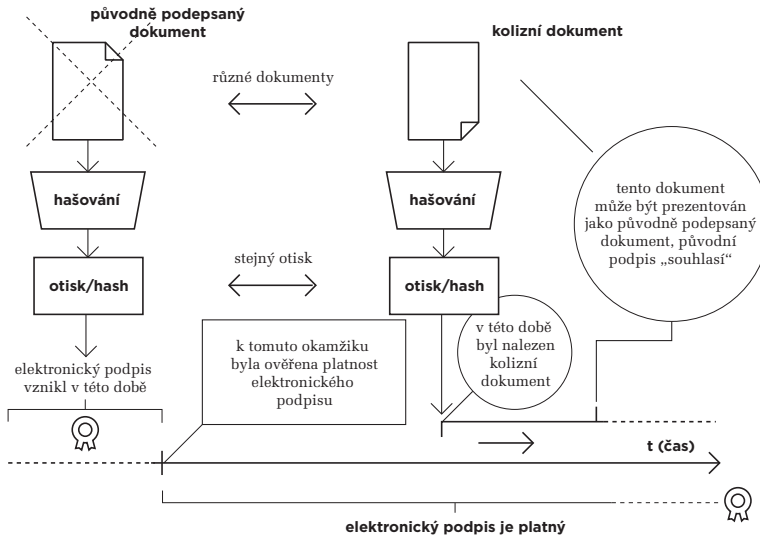
Případné porušení integrity ale ošetříme relativně snadno. Vlastně ho už máme ošetřené, a to právě tím elektronickým podpisem, jehož platnost zkoumáme. Protože porušení integrity zjistíme při vyhodnocování platnosti (ověřování) tohoto podpisu nezávisle na době, kdy tak činíme. Tedy bez ohledu na to, zda již skončila platnost příslušného podpisového certifikátu či ještě nikoli.

Problém je ale v něčem jiném: v mezidobí, od vzniku podpisu do aktuálního okamžiku, kdy integritu vyhodnocujeme, mohlo dojít k takovému vývoji v oblasti kryptografie a růstu výpočetní kapacity, že již je možné reálně nalézt (vypočítat) k danému dokumentu nějaký kolizní dokument. Pokud bychom k tomuto koliznímu dokumentu připojili původní elektronický podpis (podpis původního dokumentu), pak bychom vůbec neodhalili, že jde o kolizní dokument – protože vyhodnocení platnosti podpisu by nevykázalo porušenou integritu.

Obdobné nebezpečí, byť s menší pravděpodobností, pak hrozí i certifikátu, ze kterého by se v aktuálním čase ověřovala neporušenost integrity. Protože kdyby k němu někdo dokázal najít kolizní dokument (kolizní certifikát), byl by tím podvržen i veřejný klíč, obsažený v certifikátu.

Obrázek 4-25

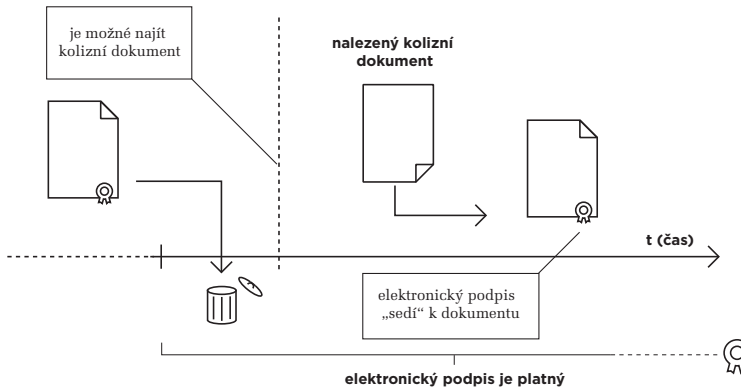
Nebezpečí, vyplývající z existence kolizního dokumentu



Čeho se tedy potřebujeme vyvarovat, je nebezpečí, které ukazuje následující obrázek: že nám někdo časem vymění původně podepsaný dokument za jiný (za nějaký kolizní dokument), ponechá u něj původní elektronický podpis a bude tvrdit, že jde o původní a řádně podepsaný dokument. Bude-li za této situace provedeno ověření podpisu, může skončit výsledkem „ano“ a my nebudeme mít jak prokázat, že nejde o původní dokument. Nebo ani nebudeme tušit, že nejde o původní dokument (když elektronický podpis bude „sedět“).

Obrázek 4-26

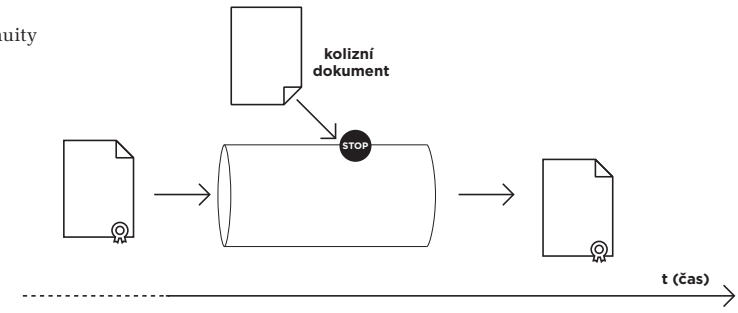
Představa narušení kontinuity kolizním dokumentem



Princip obrany proti takovémuto nebezpečí je v zásadě jednoduchý: musíme původní dokument „zafixovat“ tak, aby jej nikdo nemohl nahradit jiným (kolizním) dokumentem. A to ani v době (či spíše: hlavně v době), kdy už bude možné reálně nalézt (vypočítat) nějaký kolizní dokument.

Můžeme si to představit (v souladu s následujícím obrázkem) jako vytvoření jakéhosi „tunelu“ kolem původního dokumentu, který zabrání jeho záměně jiným dokumentem.

Obrázek 4-27
Představa principu zachování kontinuity („zafixováním“ dokumentu)



4.10.2.1 Řešení s přerazítkováváním

Jednou z možností, jak dosáhnout požadovaného efektu tunelu z předchozího obrázku, je nové podepsání již jednou podepsaného dokumentu (tj. přidání dalšího elektronického podpisu), ještě než skončí platnost certifikátu, na kterém je založen původní podpis.[42] A pak případně přidání dalšího a dalšího podpisu, ve vhodné časové posloupnosti.

Opakovaným podepisováním totiž můžeme reagovat na průběžné „zastarávání“ kryptografických algoritmů a kompenzovat je použitím nových a silnějších šifer i větších klíčů (v rámci nově přidávaných podpisů). Vždy tak, aby se adekvátně zvýšila náročnost nalezení kolizního dokumentu (a zůstávala stále dostatečně nad aktuálními možnostmi výpočetní techniky).

Přidávání dalších elektronických podpisů by skutečně problém řešilo, ale jen po technické stránce. Mohlo by ale způsobit jiný problém po stránce právní. Podpis na dokumentu by totiž mohl být chápán jako souhlas s jeho obsahem. A to nemusí korelovat s tím, že podpis přidává někdo, kdo se k obsahu podepsaného dokumentu vyjadřovat nechce. Třeba někdo, kdo provozuje dlouhodobý archiv elektronických dokumentů, s jejichž obsahem nemá sám nic společného.

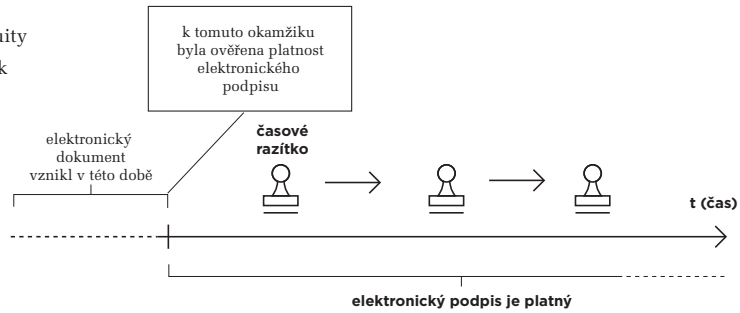
[42] Protože platnost certifikátu je zcela záměrně nastavována tak, aby se včas předešlo možnosti nalézt kolizní dokument.

Právně čisté je přidávání časových razítek, které skutečně plní pouze roli „zafixování v čase“, bez jakéhokoli dalšího vyjádření k samotnému obsahu podepsaného dokumentu.

Jenže ani časové razítko není imunní vůči hrozbě kolizních dokumentů, a proto i ono je založeno na certifikátu, který má omezenou „životnost“ v čase (byť typicky několikanásobně delší, než u elektronických podpisů). Ale stále tak krátké, aby se předešlo možnosti vzniku kolizních dokumentů. Proto i u časového razítka můžeme ověřit jeho platnost také jen po určitou omezenou dobu (po dobu řádné platnosti certifikátu, obvykle do tří či pěti let).

Takže pro možnost zajištění digitální kontinuity na delší časová období je vhodné původní časové razítko překrýt novým časovým razítkem ještě dříve, než skončí platnost certifikátu původního razítka – a takovéto „přerazítkovávání“ podle potřeby opakovat tolikrát, kolikrát je třeba. Představu ukazuje následující obrázek.

Obrázek 4-28
Představa zachování digitální kontinuity pomocí posloupnosti časových razítek



4.10.2.2 Řešení s důvěryhodnou úschovou

Jinou možností, jak dosáhnout požadovaného efektu „tunelu“, je svěřit původní dokument do úschovy někomu, kdo se o něj dokáže postarat – a kdo nám jej i po delší době vrátí s vlastním dobrozdáním, že jde stále o původní dokument.

Ve světě listinných dokumentů takto funguje například notářská úschova:[43] notář v určitém časovém okamžiku převezme dokument, průběžně ho uchovává a po čase ho zase vydá. Přitom odpovídá za jeho autenticitu (že jde o původní dokument), a při jeho vydávání zpět je také oprávněn vydat své dobrozdání o tom, že jde o původní dokument. Toto jeho dobrozdání má právní relevanci, tj. osvědčuje autentičnost dokumentu – protože notářská úschova má oporu v zákoně.

V případě elektronických dokumentů by se mohlo jednat o služby jakéhosi „elektronického notáře“. Ten by přebíral do své úschovy elektronické dokumenty, a v okamžiku jejich převzetí by ověřoval elektronické podpisy na těchto dokumentech. Pak by dokumenty uchovával – a v okamžiku jejich vydávání by dával své dobrozdání o tom, že v době převzetí dokumentu byl podpis na dokumentu platný.

Toto jeho dobrozdání by mohlo mít podobu elektronického podpisu (podpisu notáře), přidávaného k dokumentu (jako další podpis) v okamžiku vydávání dokumentu z úschovy. A pokud by funkce elektronického notáře byla vhodně ukotvena v zákoně, mohlo by toto jeho dobrozdání (ve formě podpisu) současně ověřovat a dokládat platnost původního podpisu na dokumentu.

Samozřejmě by se nemuselo nutně jednat o elektronického notáře, ale o jakýkoli archiv elektronických dokumentů – který by splňoval zákonem stanovené podmínky, aby jeho dobrozdání (při výdeji dokumentu z archivu) mohlo prokazovat platnost původního podpisu.

4.10.2.3 Řešení na bázi vyvratitelné domněnky pravosti

Další možností, která bývá v praxi také prezentována jako řešení digitální kontinuity, je aplikace dosti specifického ustanovení v zákoně o archivnictví,[44] který ve svém §69a, článku 8 obsahuje následující pasáž:

> *Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentů a opatřen kvalifikovaným časovým razítkem. Ustanovení věty první se vztahuje i na dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.*

Toto ustanovení, neformálně označované jako **vyvratitelná domněnka pravosti**, primárně řeší „pravost“ podepsaného dokumentu, a nikoli platnost podpisu na něm. Má podobu implikace: jsou-li splněny určité předpoklady („byl-li dokument podepsán, resp. opatřen značkou ….“), vyplývá z nich určitý důsledek („dokument … se považuje za pravý“). Tento důsledek je ale opatřen zpochybněním, v podobě formulace „dokud se neprokáže opak …“.

Pokud se na toto ustanovení podíváme z čistě věcného pohledu, pak vlastně nic nového nepřináší. Pokud totiž dokážeme spolehlivě prokázat platnost jeho předpokladů, měl by z nich stejný důsledek vyplývat již ze samotné podstaty elektronického podpisu a z toho, že podpisy (včetně těch elektronických) neztrácí svou platnost v čase.

Jinými slovy: pokud jsme stále ještě schopni ověřit, že elektronický podpis na dokumentu je platný (k posuzovanému okamžiku v současnosti či někdy v minulosti), pak z neomezené platnosti elektronických podpisů v čase (viz výše) vyplývá, že podpis na dokumentu je platný i nadále. Současně nám tato možnost ověření dává jistotu i ohledně toho, že jde o ten samý dokument – protože součástí

---

43 Obdobně funguje též soudní či úřední úschova.

44 Zákon č. 499/2004 Sb., o archivnictví a spisové službě.

(kladného) ověření platnosti je i zjištění, že nebyla porušena integrita. A to, že jsme stále ještě schopni řádně ověřit platnost podpisu, nás chrání i proti nebezpečí existence kolizních dokumentů.

Pak ale nepotřebujeme žádnou domněnku pravosti (navíc opatřenou oním zpochybněním, v podobě „dokud se neprokáže opak …"), protože pravost dokumentu již jednoznačně vyplývá z naší schopnosti ověřit platnost podpisu na dokumentu.

No a pokud již nejsme schopni ověřit platnost podpisu na dokumentu, pak nám vyvratitelná domněnka pravosti stejně nepomůže. Nemůžeme ji aplikovat, protože nedokážeme prokázat splnění jejích předpokladů (že dokument byl opatřen platným podpisem či značkou).

Proč ale potom uvedená „vyvratitelná domněnka pravosti" vůbec existuje? Proč ji někdo zahrnul do platné legislativy?

Možné vysvětlení by se nabízelo v případě, pokud bychom popřeli tezi, že elektronické (ale i jiné) podpisy si zachovávají svou platnost v čase trvale a bez ohledu na to, zda ještě jsme či již nejsme schopni jejich platnost ověřit.

Pokud bychom místo toho přijali opačnou tezi (že platnost elektronického podpisu končí, jakmile přestaneme být schopni ji prokázat řádným ověřením), pak by uvedená domněnka cosi přinášela: vlastně by říkala, že můžeme věřit v pravost dokumentu, i když už podpis na něm přišel o svou platnost (a my jeho dřívější platnost prokážeme nějak jinak, například skrze nějaký důvěryhodný záznam).

Na první pohled je to logické, ale na druhý již nikoli: budeme-li věřit dokumentu, i když už nejsme schopni řádně ověřit platnost jeho podpisu (či značky), pak nejsme chráněni proti nebezpečí kolizních dokumentů. A samotná domněnka by dokonce říkala, že máme věřit případnému koliznímu dokumentu (dokud někdo neprokáže, že jde o jiný dokument, než ten původní).

4.10.2.4 Proč to s elektronickými podpisy není stejné, jako s vlastnoručními?

Zůstaňme ještě na chvíli u popisované domněnky a povšimněme si její „vyvratitelnosti". Tedy odkazu na to, že „něco platí, dokud se neprokáže opak". Jde totiž o princip, který ukazuje na jeden velmi významný rozdíl mezi elektronickým a vlastnoručním podpisem.

Ve světě klasických (vlastnoručních) podpisů se s tímto principem vcelku běžně pracuje. Byť není nikde formulován a zakotven, ale jde spíše o obvyklou praxi: že platnost (či „pravost") vlastnoručních podpisů na listinných dokumentech se skutečně zkoumá obvykle až v okamžiku, kdy je někdo zpochybní. Nikoli „dopředu", v okamžiku kdy někdo někomu předkládá nějaký (vlastnoručně) podepsaný listinný dokument.[45]

Ve světě elektronických podpisů je tomu ale jinak. Zde existuje konkrétní důvod, kvůli kterému je nutné ověřovat platnost elektronických podpisů „dopředu" a nikoli až poté, kdy je někdo zpochybní.

Tímto důvodem je právní úprava, která přenáší odpovědnost za případné škody na toho, kdo se spoléhá na platnost podpisu (spoléhající se stranu, resp. spoléhající se osobu), ale neprovedl všechny úkony potřebné k tomu, aby si tuto platnost ověřil.

Jde konkrétně o ustanovení zákona č. 227/2000 Sb. (o elektronickém podpisu) a jeho paragrafu 5, který ve svém odstavci 1 nejprve řeší odpovědnost podepisující osoby. Tedy toho, kdo má ve svém držení (svůj) soukromý klíč a měl by se o něj starat tak, aby nedošlo k jeho zneužití. A pokud by snad ke zneužití došlo, má podepisující osoba povinnost využít možnost revokace a vyžádat si předčasné zneplatnění (revokaci) svého certifikátu:

1. *Podepisující osoba je povinna*
   a) *zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,*
   b) *uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.*

Další odstavec pak řeší odpovědnost za škody, vzniklé v důsledku porušení těchto povinnosti (definovaných v odstavci 1). Odpovědnost primárně ukládá podepisující osobě (držiteli soukromého klíče). Současně ale řeší i možnost, že zavinění je naopak na spoléhající se straně (přesněji: na tom, komu vznikla škoda), která neudělala vše potřebné pro ověření platnosti podpisu:

2. *Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.*

Spoléhající se strana například vůbec nemusela vyhodnotit platnost podpisu – a díky tomu nezjistila, že byla porušena integrita podepsaného dokumentu (což implikuje neplatnost podpisu). Nebo nemusela zkontrolovat, zda podpisový certifikát nebyl zneplatněn (což také implikuje neplatnost podpisu).

Pokud tedy spoléhající se strana neudělala všechny potřebné úkony k ověření podpisu – a to ještě před tím, než se začala spoléhat na platnost podpisu a podle toho jednat – pak odpovědnost nenese podepsaná strana. A škoda tak zůstává na tom, komu vznikla.

---

45 Správně bychom ale měli rozlišovat mezi veřejnými listinami, u kterých platí presumpce pravosti a správnosti, a soukromo-právními dokumenty, u kterých takováto presumpce neplatí a je na předkladateli, aby prokázal jejich pravost a správnost.

4.10.3 Elektronické podpisy s možností ověření i po dlouhé době

Snaha o zachování „digitální kontinuity“, chápané jako možnost ověřit platnost konkrétního podpisu i libovolně dlouho po vzniku tohoto podpisu, však v praxi naráží ještě na další problémy, než jsou ty popsané v předchozích odstavcích.

Například časové razítko (či správně aplikovaná posloupnost časových razítek) nám „fixuje“ určitý dokument v čase a dává nám jistotu, že se od příslušné doby nezměnil. Chrání nás tak i před nebezpečím kolizních dokumentů. V případě, kdy jde o dokument s interním elektronickým podpisem, současně takto chrání i samotný podpis, nacházející se „uvnitř“ dokumentu.

Jenže neměnnost původního dokumentu (a jeho podpisu) nám nemusí stačit k tomu, abychom i v současnosti mohli spolehlivě ověřit platnost podpisu na dokumentu, byť k nějakému staršímu posuzovanému okamžiku.

4.10.3.1 Koncept LTV (Long Term Validation)

Jak už víme z kapitoly 3, k (pozitivnímu) ověření platnosti potřebujeme i určité „externí“ informace. Konkrétně samotný certifikát, na kterém je zkoumaný podpis založen, dále všechny jeho nadřazené certifikáty (na příslušné certifikační cestě), a také informace o stavu revokace všech těchto certifikátů. A teď to nejpodstatnější: tyto informace musí být vztaženy k době, ke které platnost podpisu ověřujeme. Tedy k příslušnému posuzovanému okamžiku.

Samotné certifikáty (ať již ten „podpisový“ či jeho nadřazené certifikáty) mohou, ale také nemusí být vloženy přímo do podepsaného dokumentu (v případě interního podpisu), nebo začleněny do externího podpisu – tak aby byly k dispozici v okamžiku, kdy je podpis ověřován.

Ale největší problém bývá s nezbytnými informacemi o stavu revokace všech těchto certifikátů, ať již se jedná o informace získávané „dávkově“, skrze seznamy CRL nebo „interaktivně“, skrze protokol OCSP. Připomeňme si, že v rámci ověřování musíme vždy zkontrolovat, zda nedošlo k revokaci (předčasnému zneplatnění) některého z těchto certifikátů ještě v době jeho řádné platnosti. Pokud ale k ověření dochází po delší době od vzniku podpisu – a hlavně od skončení řádné platnosti samotných certifikátů – nemusí být takováto informace již dostupná.

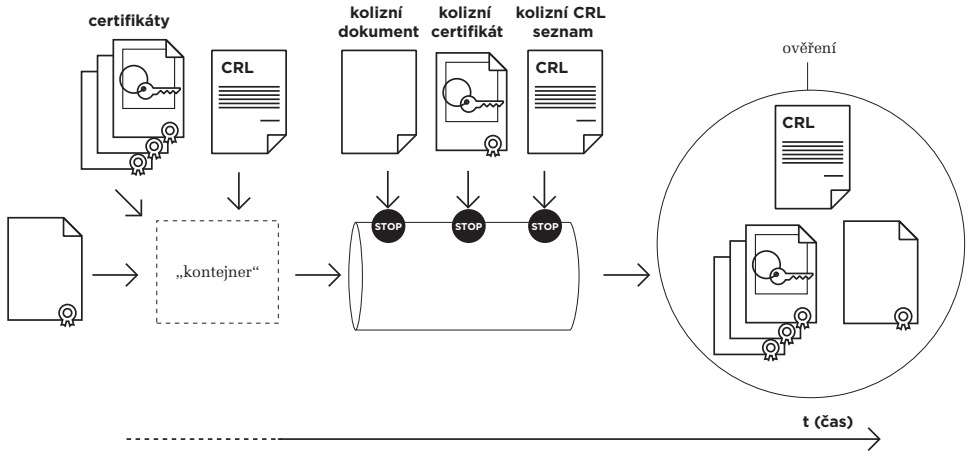
Jak jsme si již uvedli v části 3.4.4, informace o revokaci se ze seznamu CRL „vytrácí“ (přestává v nich být obsažena) ihned, jakmile skončí řádná platnost certifikátu. Tedy alespoň u „intervalových“ seznamů CRL, se kterými pracuje většina certifikačních autorit.

Řešením může být to, že k podepsanému dokumentu (a jeho podpisu) se kromě samotného podpisu, časového razítka či razítek a všech relevantních certifikátů „přibalí“ také příslušná informace o stavu revokace certifikátů. Tak aby ten, kdo bude kdykoli později ověřovat platnost podpisu, měl všechny potřebné údaje k dispozici.

Představu ukazuje následující obrázek:

Obrázek 4-29

Představa podpisů s možností ověření i po delší době



Výsledkem je koncept, označovaný jako „Long Term Validation“, resp. LTV. Umožňuje ověřovat platnost elektronických podpisů i po delší — či dokonce „hodně dlouhé“ — době.

Samozřejmě ale i takovýto postup má svá úskalí. Například v tom, že informace o stavu revokace certifikátů, která by se vztahovala k okamžiku vzniku podpisu (resp. k okamžiku na časovém razítku), bývá k dispozici až o něco později (například až se dostane na seznamy CRL, což může obnášet zpoždění až 24 hodin). Takže takovouto informaci má smysl připojovat k vytvořenému podpisu „až po nějakém čase“, aby se tyto závislosti zohlednily.

4.10.3.2 „Pokročilé“ elektronické podpisy – CadES, XAdES a PAdES

Pro praktickou implementaci konceptu LTV je třeba navrhnout, standardizovat a implementovat jednotný způsob, jakým by se všechny potřebné informace (počínaje certifikáty, přes časová razítka, až po informace o revokaci) k podepisovaným dokumentům „přibalily“. A to tak, aby to bylo dostatečně důvěryhodné a spolehlivé, a mohlo tak být podkladem k takovému (pozdějšímu) ověření platnosti podpisu, které by splňovalo i všechny požadavky kladené zákonem.

V současné době (od roku 2008 a 2009) existuje dokonce několik vzájemně souvisejících standardů, popisujících jak toho docílit. Společně jsou označovány jako „pokročilé“ elektronické podpisy (v angličtině: „Advanced Electronic Signatures“). Liší se především v tom, pro jaké druhy podepisovaných dokumentů či objektů jsou určeny:

- **CAdES** (CMS Advanced Electronic Signatures), pro podepisování (jakýchkoli) objektů
- **XAdES** (XML Advanced Electronic Signatures), pro podepisování XML dokumentů
- **PAdES** (PDF Advanced Electronic Signatures), pro podepisování PDF dokumentů

Podstatné přitom je, že všechny tyto koncepty (resp. „rámce“) jsou určitým způsobem odstupňovány) podle toho, co a jak je k samotnému podpisu „přibaleno“ – zda časové razítko, certifikáty z celé certifikační cesty, informace o revokaci, či jen odkazy na tyto informace, případně více časových razítek atd. Tak například u XAdES podpisů (v XML dokumentech) se hovoří o těchto úrovních:

- **základní úroveň:** představuje jen „základní“ elektronický podpis (bez časového razítka a dalších informací). Umožňuje ověřit platnost podpisu pouze po dobu řádné platnosti certifikátu, na kterém je podpis založen. Fakticky jde o „původní“ podpis bez jakéhokoli rozšíření.
- **úroveň XAdES-T (Timestamp):** na této úrovni je k elektronickému podpisu připojeno časové razítko – a příslušný koncept na této úrovni definuje konkrétní způsob, jakým má být časové razítko k podpisu připojeno
- **úroveň XAdES-C (Complete):** na této úrovni jsou k podpisu připojeny odkazy na všechny certifikáty na certifikační cestě a odkazy na všechny revokační informace. Nikoli ale tyto informace jako takové (ale pouze odkazy na ně).
- **úroveň XAdES-X (eXtended):** na této úrovni jsou k podpisu kromě odkazů na certifikáty na certifikační cestě a na revokační informace (jako u úrovně C) připojena ještě časová razítka, pokrývající tyto certifikáty a revokační údaje (čímž je zabráněno jejich eventuální záměně)
- **úroveň XAdES-X-L (eXtended Long term):** na této úrovni jsou k podpisu připojeny samotné certifikáty na certifikační cestě a revokační informace (a nikoli jen odkazy na ně).
- **úroveň XAdES-A (Archival):** na této úrovni může být k podpisu přidávána ještě posloupnost dalších časových razítek, které zajišťují dlouhodobou kontinuitu (ve smyslu předchozího textu a obrázku 4.26)

Podpora XAdES a jeho jednotlivých úrovní se přitom prosazuje do praxe (a do konkrétních produktů) jen postupně (a bohužel dosti pomalu). Jak uvidíme v kapitole 7, XAdES již podporuje například kancelářský balík MS Office, ovšem teprve od verze 2010.

V případě PAdES podpisů (na PDF dokumentech) se hovoří jednak o profilech (které představují varianty PAdES podpisů), a jednak o „částech“ (parts), které popisují konkrétní část standardu:[46]

- **PAdES Overview** (část 1): je celkovým přehledem PAdES, ještě nepopisuje konkrétní profily
- **PAdES Basic** (část 2): jde o část standardu, popisující „původní“ podpisy[47] na PDF dokumentech. Řeší jak prodlužovat možnost jejich ověření, pomocí přidávání časových razítek a revokačních informací k těmto podpisům. Ještě ale neumožňuje přidávat samostatná („archivní“) časová razítka.
- **PAdES Enhanced** (část 3): tato část standardu zavádí profily, založené na konceptu CAdES. Konkrétně na CAdES-BES (pak jde o profil PAdES-BES), který může být doplněn samostatným (archivním) časovým razítkem (profil PAdES-T), a dále profil CAdES-EPES. V něm může být

k podpisům připojena také informace o tom, v rámci jakého kontextu („podpisové politiky“) jsou podpisy vytvářeny a vyhodnocovány.

- **PAdES Long Term** (část 4): tato část definuje profil PAdES-LTV (někdy označovaný také jako PAdES-A), který již umožňuje postupně přidávat k podpisu posloupnost časových razítek, za účelem zajištění časové kontinuity (ve výše uvedeném smyslu).
- **PAdES for XML Content** (část 5): v tomto profilu lze přidávat posloupnost časových razítek k XML obsahu v rámci PDF dokumentu (například k polím formuláře, určeným k vyplňování).

Konkrétní nástroje pro práci s PDF dokumenty nejčastěji podporují jen „původní“ PDF podpisy, které v rámci PAdES odpovídají části 2, resp. profilu Basic.

Ostatní profily, resp. části (3 až 5), jsou zatím implementovány jen výjimečně. Většina producentů příslušných nástrojů nejspíše čeká na to, že se tyto profily stanou součástí nového standardu ISO 32000-2.[48]

Konkrétně u produktů společnosti Adobe je podpora PAdES na úrovni 3 až 4 zavedena v řadě X (Adobe Acrobatu X a Readeru X). Produkty verze 9 (Acrobat 9 a Reader 9) ještě podporují pouze PAdES do úrovně 2 (včetně). Podrobněji viz kapitola 6.

---

46 Standardu ETSI 102 778, který by měl být v budoucnu zapracován do nového standardu ISO 32000-2.

47 Tak, jak je definuje norma ISO 32000-1 z roku 2008.

48 Jeho vydání se očekává koncem roku 2011, případně až v roce 2012.

Úroveň III — Praxe

5. Elektronický podpis v počítači

Kapitola 5

5. Elektronický podpis v počítači

Jako koncoví uživatelé chceme pracovat s elektronickým podpisem zcela rutinně. A to jak ověřovat platnost elektronických podpisů (či elektronických značek a časových razítek), které vytvořil někdo jiný, tak i vytvářet své vlastní elektronické podpisy na nejrůznějších elektronických dokumentech či zprávách. Případně využívat postupy, metody a technologie elektronického podpisu k dalším činnostem, například k šifrování, k bezpečnému přihlašování apod.

Všechny tyto činnosti přitom mohou být na námi používaných počítačích maximálně usnadněny, při zachování nezbytných zásad bezpečnosti. V zásadě může být vše zredukováno jen na jediné kliknutí (a ověření, skrze zadání zabezpečujícího údaje, například hesla či PINu, při vytváření podpisu).

Jenže takovéto maximální zjednodušení může být až určitou třešničkou na dortu, kterému musí předcházet pečlivá příprava. A to jak naše vlastní příprava, charakteru osvěty (abychom správně rozuměli tomu, co všechno se na náš pokyn provede), tak i příprava našeho počítače a všech jeho součástí, které jsou k práci s elektronickými podpisy používány. V neposlední řadě je nutnou součástí přípravy i získání potřebných certifikátů, které chceme při práci s elektronickými podpisy využívat.

Právě těmto aspektům bude věnována tato kapitola. Řekneme si v ní, jak konkrétně postupovat, když si chceme nechat vystavit vlastní certifikát. Dále si naznačíme, jak se s certifikáty a dalšími náležitostmi pracuje na našem počítači – jak si nainstalovat čipovou kartu či USB token, jak je zpřístupnit aplikacím, které by s nimi měly pracovat či jak a kam instalovat cizí i své vlastní certifikáty.

Vše si budeme ukazovat v prostředí operačního systému MS Windows, verze XP s SP3 nebo vyšší. To proto, že jde o variantu operačního systému, která je mezi širší uživatelskou veřejností zdaleka nejrozšířenější. V jiných operačních systémech jsou základní principy práce s elektronickým podpisem samozřejmě stejné, ale některé implementační detaily se mohou lišit.

5.1 Úložiště certifikátů

Již v první kapitole jsme se seznámili s některými základními pojmy, které jsme si v dalších kapitolách upřesňovali. Zde se nevyhneme jejich připomenutí, ale také upřesnění a hlavně zavedení zcela nových pojmů a souvislostí.

Ze všeho nejprve si připomeňme, že certifikáty jsou ukládány do tzv. **úložiště (úložiště certifikátů,** anglicky **Certificate Store**, zkratkou **CS**). Spíše bychom jej ale mohli považovat za „úložiště důvěryhodných certifikátů“, protože (až na malé výjimky, viz část 5.4.2.3) vložení konkrétního certifikátu do úložiště znamená, že je mu vyjádřena důvěra.

Úložiště (důvěryhodných) certifikátů přitom nemusí být na našem počítači zdaleka jen jedno. Naopak, bývá jich více. Dokonce můžeme vyjít z představy, že každá aplikace používá vlastní úložiště certifikátů a pak být příjemně překvapeni, že některé aplikace dokáží nějaké úložiště sdílet.

> V prostředí MS Windows existuje „systémové“ úložiště certifikátů, které je společně sdíleno aplikacemi z produkce společnosti Microsoft, například prohlížečem Internet Explorer či programy z kancelářského balíku MS Office. Ale třeba Adobe Reader již má vlastní úložiště, nicméně (na vyžádání) je schopen využívat i to „systémové“ v operačním systému MS Windows. Jiným příkladem může být prohlížeč Mozilla Firefox, který také používá vlastní úložiště certifikátů a není schopen sdílet to „systémové“.

Existence různých úložišť certifikátů je přitom nesmírně důležitá (a doslova klíčová) i z čistě uživatelského pohledu. Každá aplikace totiž bude považovat za důvěryhodné právě a pouze ty certifikáty, které jsou obsaženy v tom úložišti, se kterým pracuje.

> Pokud například vyjádříme svou důvěru všem kořenovým certifikátům CA PostSignum, a to tak, že je nainstalujeme do úložiště certifikátů Firefoxu, bude tento prohlížeč považovat za důvěryhodné všechny servery, vybavené certifikátem od této certifikační autority (obecně všechny certifikáty, ke kterým existuje certifikační cesta k příslušnému kořenovému certifikátu). Ale Internet Explorer, který používá jiné úložiště certifikátů než Firefox, v takovém případě nebude mít podle čeho posoudit jejich důvěryhodnost, a tak bude před jejich návštěvou varovat.

5.1.1 Vlastní certifikáty vs. certifikáty třetích stran

Nejčastěji budeme chtít vyjadřovat svou důvěru kořenovým certifikátům konkrétních certifikačních autorit, a právě ty ukládat do úložišť důvěryhodných certifikátů. Díky principům infrastruktury veřejného klíče (hlavně principu delegace důvěry) tím vždy vyjádříme důvěru celému „podstromu“, neboli všem certifikátům, vydaným danou certifikační autoritou.

Někdy ale můžeme udělat výjimku a vyjádřit svou důvěru i konkrétním certifikátům, bez ohledu na jejich příslušnost do nějakého konkrétního „stromu důvěry“. Tedy například konkrétnímu serverovému certifikátu či osobnímu certifikátu konkrétní osoby apod. Nebo nějakému certifikátu s vlastním podpisem (self-signed), který není kořenovým certifikátem certifikační autority. Vždy samozřejmě jen za podmínky, že máme proč těmto certifikátům důvěřovat.

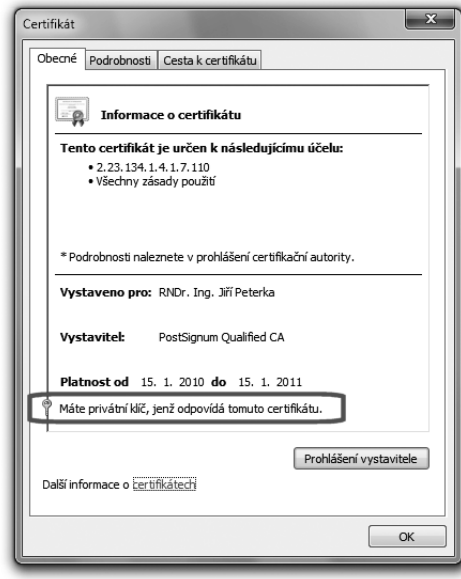
Všechny tyto certifikáty ale budou certifikáty třetích stran, a nikoli „naše“. Jsou to certifikáty plně veřejné, a my je budeme využívat pouze pro vyhodnocování platnosti (cizích) podpisů, značek či razítek. Proto na spolehlivost jejich uložení nejsou kladeny žádné zvýšené požadavky.[1] A důvěrnost tohoto uložení (tj. aby je nemohl získat někdo jiný) již není zapotřebí vůbec.

Přesně opačné to je v případě našich vlastních certifikátů, které chceme využívat při vytváření našich elektronických podpisů či dokonce značek. Tyto certifikáty jsou samy o sobě veřejné, takže jejich kompromitace by nás také nemusela nijak bolet. Ale problém je v tom, že spolu s těmito certifikáty si do úložišť potřebujeme ukládat i jim odpovídající soukromé klíče.

---

[1] Na rozdíl od „správnosti“ jejich uložení: je třeba je uložit na správné místo do správného úložiště certifikátů.

Obrázek 5-1
Příklad certifikátu, se kterým je v úložišti uložen i odpovídající soukromý klíč



A tady jsou již nároky na spolehlivost a důvěrnost uložení naopak velmi vysoké, protože případná kompromitace soukromého klíče (jeho zkopírování, smazání apod.) by byla zcela zásadním problémem.[2]

Určitým řešením je aplikování zvýšené ochrany soukromého klíče v úložišti, která se uplatňuje v situacích, kdy má být se soukromým klíčem nějak manipulováno. Tedy při vytváření konkrétního elektronického podpisu.

V prostředí MS Windows máme k dispozici tři různé úrovně ochrany soukromého klíče, mezi kterými můžeme volit:

- **vysoká úroveň:** při každém požadavku na použití soukromého klíče bude nutná autentizace (zadání správného hesla)
- **střední úroveň:** každý požadavek na použití soukromého klíče je nutné explicitně odsouhlasit (odkliknout, ale bez nutnosti zadání hesla)
- **nízká úroveň:** při použití soukromého klíče nebude vyžadována žádná akce uživatele

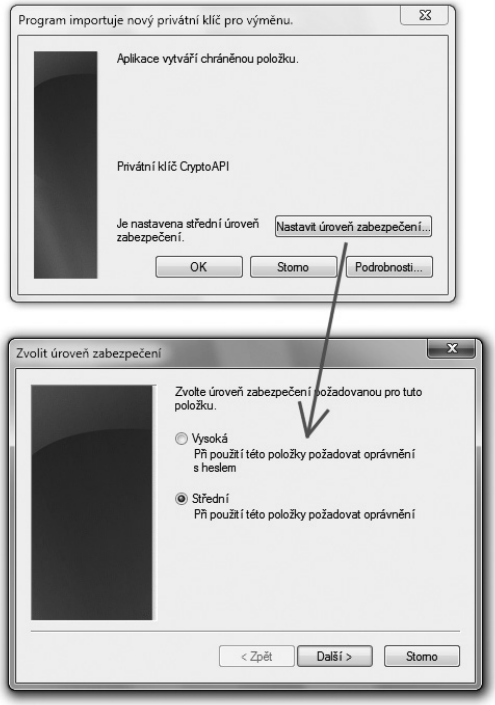
Nastavení těchto úrovní, včetně volby hesla, se provádí již při prvotním generování soukromého klíče (pro potřeby žádosti o vydání certifikátu, viz část 5.5.2.2). Stejně tak se ale provádí (znovu, s novou volbou hesla) při případném vkládání (importu) certifikátu i se soukromým klíčem do jiného úložiště. Samotné nastavení je přitom dvoustupňové: nejprve se volí mezi „silnou ochranou“ (zahrnující vysokou a střední míru ochrany) a žádnou ochranou (nízkou).

[2] Byť také řešitelným, skrze předčasné zneplatnění alias revokaci.

Obrázek 5-2
Příklad povolení silnější ochrany (vysoké či střední, při instalování certifikátu spolu se soukromým klíčem)

Teprve při volbě „silné ochrany“ je následně možné volit mezi vysokou a střední mírou zabezpečení, a zadat heslo.

Obrázek 5-3
Příklad volby mezi nejvyšší a střední úrovní zabezpečení



5.1.2 Logická a fyzická úložiště

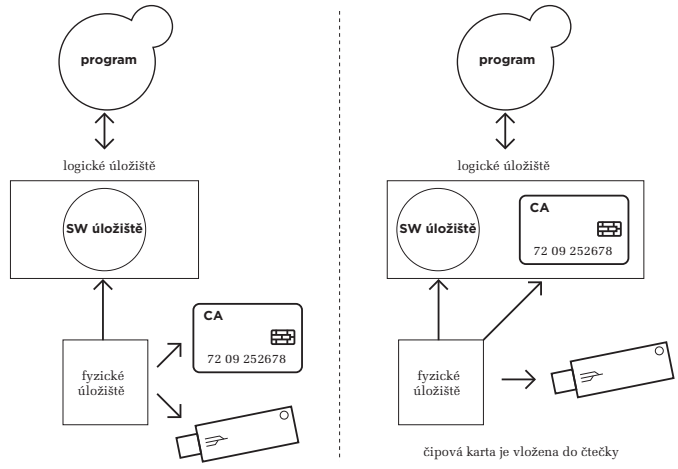
Různým požadavkům na spolehlivost a důvěrnost uložení různých certifikátů (vlastních vs. třetích stran) odpovídají i různé způsoby realizace příslušných úložišť. Pro certifikáty třetích stran jsou například plně postačující „softwarová“ úložiště, fakticky realizovaná jako soubor, uložený někde na disku našeho počítače.

Naproti tomu pro uložení osobních certifikátů, spolu s odpovídajícími soukromými klíči, jsou vhodná externí a „odnímatelná“ úložiště, realizovaná například na čipových kartách či USB tokenech.

Různé způsoby realizace úložišť nás ale nutí rozlišovat mezi „logickým“ a „fyzickým“ úložištěm. **Logickým úložištěm** je to, co „vidí“ ten program, který úložiště používá, bez ohledu na způsob realizace úložiště. Tedy bez ohledu na to, zda jde o certifikáty uložené někde na disku počítače, nebo na čipové kartě, právě vložené do příslušné čtečky či zda jde o certifikáty na USB tokenu apod.

Fyzickým úložištěm je pak onen soubor na disku, čipová karta, USB token či něco ještě jiného, co je schopné skutečně („fyzicky“) uchovávat certifikáty i s odpovídajícími klíči.

Rozdíl mezi logickým a fyzickým úložištěm je tedy i v tom, že logické úložiště je (z pohledu konkrétního programu) vždy jedno, zatímco fyzických může být více – a podle momentální situace se „skládají“ do (jednoho) logického úložiště, jak naznačuje obrázek.



Obrázek 5-4
Představa logického úložiště a fyzických úložišť

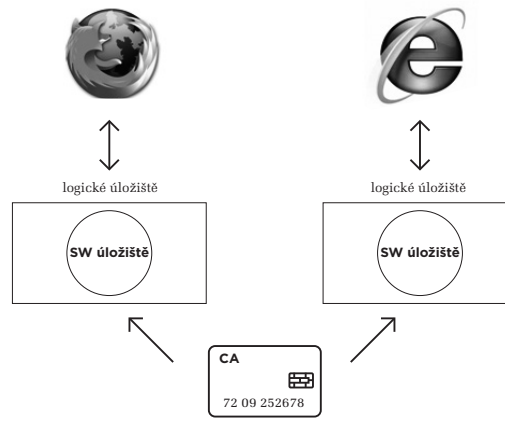
I v rámci fyzických úložišť bychom ale měli správně rozlišovat mezi těmi, které jsou „odnímatelné“ a tudíž k dispozici jen někdy (jako čipová karta či USB token), a těmi které nejsou odnímatelné a mohou tak být k dispozici kdykoli. Říkejme těm prvním **externí úložiště**, a těm druhým **interní úložiště**.

Právě zavedené označení můžeme ihned využít ke konstatování, že pro uchovávání osobních certifikátů (včetně soukromých klíčů) se jednoznačně hodí externí úložiště. Interní úložiště se ke stejnému účelu sice dají použít také, ale je to mnohem méně vhodné.

V zásadě by se dalo říci, že při alespoň trochu zvýšených požadavcích na bezpečnost je použití externích úložišť nutností.

Rozlišování mezi interními a externími úložišti (jako variantami fyzických úložišť) nám také dovoluje upřesnit náš předpoklad o tom, že každý aplikační program si obecně vytváří své vlastní interní úložiště, které současně tvoří jeho (jediné) logické úložiště.

Obrázek 5-5
Představa využití (stejného) externího úložiště různými programy



Ovšem pokud uživatel chce, může si toto logické úložiště obsahově rozšířit tím, že do něj začlení i některá externí (fyzická) úložiště. Třeba právě externí úložiště na čipové kartě či USB tokenu, ve kterém má své osobní certifikáty.

Šikovné je, že jedno a totéž externí úložiště může být využito k rozšíření (logického) úložiště různých aplikačních programů. Jinými slovy: stačí jedna čipová karta (či jeden USB token) s osobními certifikáty a klíči, a můžete tyto certifikáty (a odpovídající soukromé klíče) zpřístupnit různým programům, které je pak mohou využívat.

5.1.3 Úložiště na čipových kartách a USB tokenech

Předností externích úložišť typu čipových karet a USB tokenů přitom není jen jejich „odnímatelný“ charakter, který umožňuje vkládat je do příslušných čteček či rozhraní jen v době jejich skutečné potřeby. Další předností je možnost zkonstruovat je tak, aby byly „uzavřené do sebe“ a soukromé klíče je vůbec nemusely (ba dokonce: ani nemohly) opustit. Díky tomu si příslušné soukromé klíče nikdo nemůže zkopírovat.

Jenže to má i svou nevýhodu: aby soukromý klíč nemusel opustit příslušný USB token či čipovou kartu, musí se jeho generování i veškeré jeho používání (až po tvorbu samotného el. podpisu) odehrávat uvnitř tokenu či karty. Externí úložiště tak musí být vybaveno dostatečnou vlastní inteligencí a výpočetní kapacitou, aby zvládlo vše potřebné. V zásadě to musí být malý jednoúčelový počítač s vlastním procesorem, specializovaným na provádění kryptografických operací. Což zvyšuje jak cenu externího úložiště, tak i složitost jeho instalace a provázání s těmi aplikacemi, které mají jeho služby využívat.

> Z pohledu dříve citovaných legislativních definic tak čipová karta (či USB token) plní roli prostředku pro vytváření elektronického podpisu, a ještě i nosiče dat pro vytváření elektronických podpisů (tj. nosiče certifikátů a klíčů).

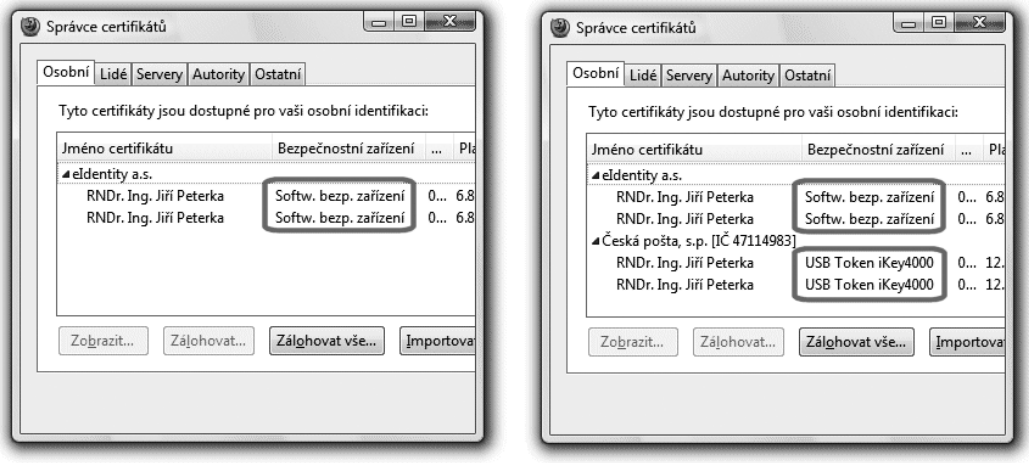
Celý problém lze shrnout tak, že interním úložištím stačí být pouhými pasivními nosiči (certifikátů a případně i soukromých klíčů), protože vše potřebné si může zajistit ta aplikace, která úložiště používá, a nepotřebuje k tomu žádnou součinnost uživatele (ve smyslu instalace nějakých ovladačů pro toto úložiště, jeho nastavení atd.). Naproti tomu u externích úložišť, které navíc nejsou zdaleka jen nějakými pasivními úložišti, ale mnohem složitějšími zařízeními s vlastní inteligencí, je situace přesně obrácená: zde je na uživateli, aby sám skloubil představy a požadavky aplikací s možnostmi příslušného zařízení a zajistil vše potřebné. Což v praxi obnáší provedení nezbytných softwarových instalací. To mnohdy není vůbec triviální, a i velmi zkušení uživatelé si na tom mohou vylámat zuby.

Přitom teprve když se vše podaří nainstalovat a zprovoznit tak, jak je potřeba, dochází ke kýženému efektu: teprve pak jsou ta externí úložiště (na čipových kartách a USB tokenech), která uživatel vložil do příslušných čteček či USB rozhraní, logicky začleněna do (logického) úložiště, používaného

Obrázek 5-6

Příklad obsahu části úložiště (prohlížeče Firefox) pro osobní certifikáty

Vlevo bez USB tokenu, vloženého do USB rozhraní, vpravo s vloženým USB tokenem



příslušným programem – a uživatel má díky tomu možnost pohodlně, jednoduše a „stejně“ pracovat i s těmi certifikáty a klíči, které se nachází na čipové kartě či tokenu.

A až uživatel skončí svou práci, kartu či token jednoduše vyjme a certifikáty i s klíči přestanou být dostupné. Tím je obsah externího úložiště zase vyřazen z logického úložiště.

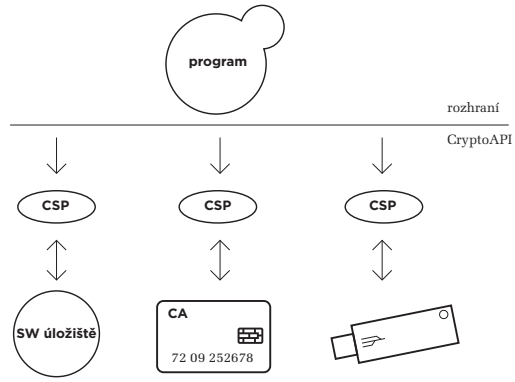
5.1.3.1 Rozhraní CryptoAPI a moduly CSP

V této knize ale rozhodně nečekejte žádný vyčerpávající návod na to, jak instalovat jakoukoli konkrétní čipovou kartu či USB token v prostředí libovolné verze MS Windows. To by bylo přinejmenším na jednu zcela samostatnou knihu

Zde se pokusíme jen o nastínění základní představy toho, jak je vše v prostředí MS Windows řešeno. A to s cílem vytvořit si určitý nadhled tak, aby zkušenější čtenář mohl alespoň tušit, o co se má snažit, a méně zkušený uživatel věděl, co přesně má požadovat po někom zkušenějším.

Svou představu můžeme odvinout od **rozhraní**, které se v prostředí MS Windows jmenuje **CryptoAPI**. Přitom API je zkratka Application Programming Interface, což znamená aplikační programové rozhraní. A prefix „Crypto“ naznačuje, že přes toto rozhraní budou jednotlivé aplikace volat konkrétní kryptografické funkce (žádat o jejich provedení). Jako třeba vytvoření otisku (hashe) nějakého dokumentu, podepsání tohoto otisku s využitím soukromého klíče atd.

Obrázek 5-7
Představa rozhraní CryptoAPI a modulů CSP



K zajištění těchto operací se „pod“ rozhraním CryptoAPI nachází **poskytovatel kryptografických služeb**, anglicky **Cryptographic Service Provider**, zkratkou **CSP**. Jde o software (softwarový modul), který zajišťuje požadované kryptografické funkce.

> Připomeňme si, že u externích úložišť typu čipových karet a USB tokenů jsou vlastní kryptografické operace prováděny „uvnitř“ úložiště, tak by soukromý klíč nemusel (resp. nemohl) úložiště opouštět.

V případě externích úložišť jsou proto (softwarové) moduly CSP spíše jen jakýmisi prostředníky, kteří pouze zprostředkovávají požadavky: přijímají je přes rozhraní CryptoAPI a zajišťují jejich provedení přímo v samotném úložišti. V případě interních úložišť tomu může být jinak a modul CSP může sám provádět konkrétní kryptografické operace s využitím klíčů, nacházejících se v úložišti.

5.1.3.2 Softwarová instalace externích úložišť

Pokud si jako uživatel pořídíte nějakou čipovou kartu, USB token či jiné obdobné zařízení, operační systém vašeho počítače nejspíše ještě nebude obsahovat potřebného poskytovatele certifikačních služeb (modul CSP), a vy mu ho musíte nejprve dodat. Je tedy na vás postarat se o instalaci potřebného softwaru.

Potřebný software by vám měl dodat výrobce vašeho zařízení. A je také na něm, jak snadná či naopak komplikovaná bude jeho instalace, a jak velké nároky na součinnosti bude vyžadovat od vás jako uživatele. V ideálním případě jen vložíte dodané CD a instalační program se již sám postará o vše potřebné.

Pro správné pochopení celého procesu instalace externích úložišť si ještě řekněme, že kromě softwarového „poskytovatele kryptografických služeb“ (modulu CSP) je obvykle třeba instalovat ještě ovladač samotného nosiče (jako hardwarového zařízení) či potřebného snímače.

> Nejlépe je to vidět na příkladu s čipovou kartou: nejprve musíte nainstalovat čtečku čipových karet. Ta se dnes připojuje nejčastěji k USB rozhraní (dříve spíše k sériovému portu), a vyžaduje instalaci příslušného softwarového ovladače. Ten se instaluje jeden (pro jednu čtečku), a díky tomuto ovladači pak počítač a jeho operační systém dokáží s danou čtečkou pracovat. Dokáží například rozpoznat, že do čtečky je či není vložena nějaká čipová karta, a pokud ano, dokáží s touto kartou komunikovat.

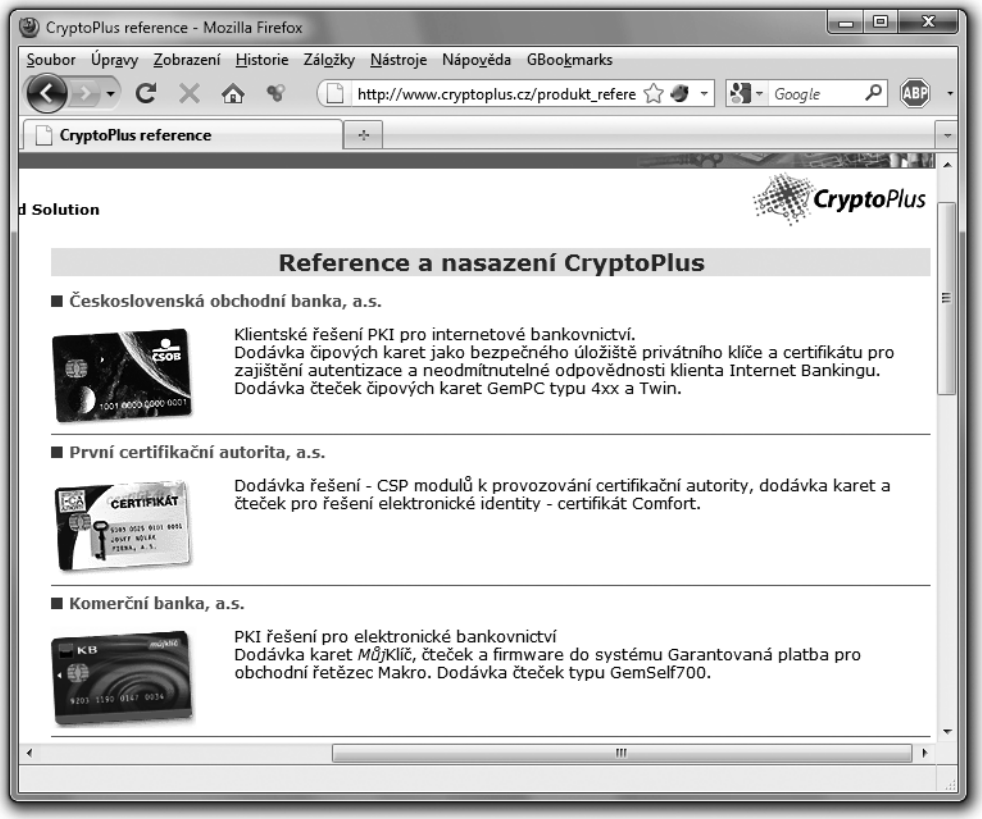
Každá čipová karta ale může „komunikovat“ jinak, ve smyslu rozsahu a způsobu poskytování svých vlastních funkcí. Takže „nad“ ovladačem čtečky čipových karet musí fungovat ještě další ovladač, který již bude rozumět konkrétní (právě vložené) čipové kartě i tomu, co tato karta nabízí a jak funguje. Tento ovladač pak kartou nabízené funkce zprostředkuje té aplikaci, která by je chtěla využívat.

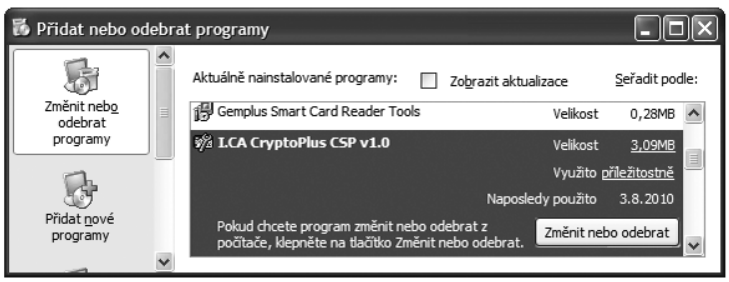
Jinými slovy: tímto dalším ovladačem, fungujícím „nad“ čtečkou čipové karty, je příslušný modul CSP, alias poskytovatel kryptografických služeb, šitý na míru konkrétní kartě.

V ČR je jako modul CSP (poskytovatel kryptografických služeb) pro čipové karty nejčastěji používán software CryptoPlus, ovšem uzpůsobený pro různé čipové karty. V rámci svého internetového bankovnictví jej používá například Česká spořitelna, Komerční banka či ČSOB, a původně jej pro své čipové karty používala i certifikační autorita I. CA.

Obrázek 5-8

Reference nasazení SW Cryptoplus



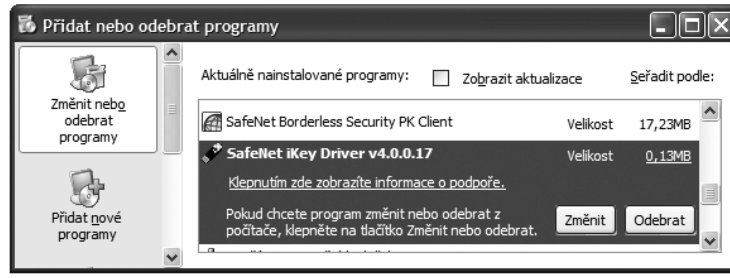


Obrázek 5-9

Příklad nainstalovaného ovladače čtečky čipových karet a CSP modulu Cryptoplus ve verzi pro I.CA

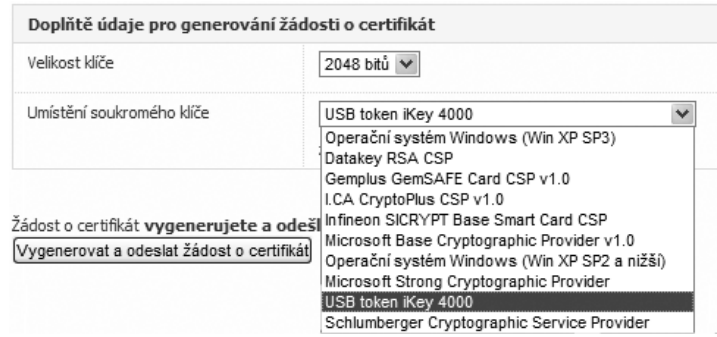
Nutnost instalovat jak ovladač zařízení, tak i další software plnící roli modulu CSP, platí i pro zařízení charakteru USB tokenů, které ale žádnou čtečku nepotřebují (nýbrž se vkládají přímo do USB portu počítače). Viz následující obrázek.

Obrázek 5-10
Příklad instalace ovladače a CSP modulu pro token iKey4000



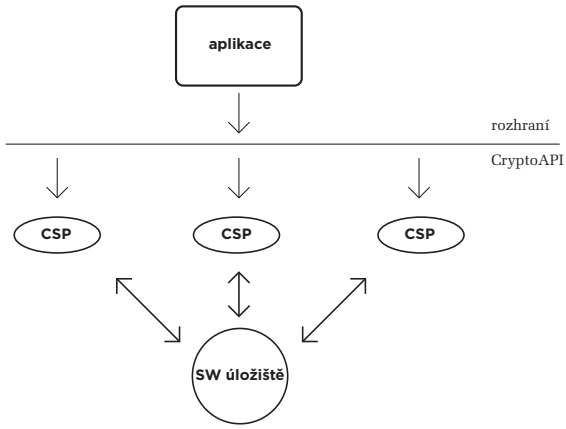
Takovýchto poskytovatelů kryptografických služeb (modulů CSP), které zprostředkovávají služby různých úložišť certifikátů, bývá i na jednom počítači více. Je to patrné i z následujícího obrázku, který ukazuje možnost výběru modulu CSP při generování žádosti o nový certifikát (viz dále) a fakticky se ptá, do kterého (fyzického) úložiště má být nový certifikát (a jemu odpovídající soukromý klíč) umístěn. Na obrázku je několik modulů CSP pro systémové „softwarové“ úložiště, několik pro čipové karty, a jeden CSP modul (ten vybraný) pro USB token iKey 4000.

Obrázek 5-11
Příklad výčtu CSP modulů



Zdůrazněme si, že k jednomu a témuž fyzickému úložišti může být k dispozici více různých modulů CSP. Týká se to hlavně interních úložišť, realizovaných softwarově (nejčastěji těch systémových, zřizovaných přímo operačním systémem), protože pouze jejich moduly CSP skutečně provádí konkrétní určité kryptografické operace.

Obrázek 5-12
Představa více modulů CSP nad jedním interním úložištěm



Moduly CSP se liší hlavně ve své „síle“: v tom, s jak velkými klíči a s jak silnými kryptografickými algoritmy, včetně hašovacích funkcí, mohou pracovat. A v závislosti na tom pak na ně mohou být, nebo naopak nemusí být, aplikována případná exportní omezení. To je i důvod existence více standardních CSP (Cryptographic Service Provider) modulů v dřívějších verzích operačního systému MS Windows:

- **Microsoft Base Cryptographic Service Provider** nepodléhá exportním omezením ze strany USA, protože je schopen pracovat jen s krátkými klíči a slabými kryptografickými algoritmy
- **Microsoft Enhanced Cryptographic Service Provider** již může podléhat exportním omezením (ze strany USA), protože dokáže pracovat s delšími klíči a silnějšími algoritmy.

Ani jeden z těchto dvou „standardních“ modulů však nedokáže pracovat s hašovacími funkcemi SHA-2,[3] které jsou dnes již (u kvalifikovaných certifikátů) povinné. Tuto schopnost má až následující CSP modul od Microsoftu:

- **Microsoft Enhanced RSA and AES Cryptographic Provider**[4]

Pokud jde o CSP moduly, instalované spolu s konkrétními čipovými kartami či USB tokeny (obecně s externími úložišti), zde je podpora SHA-2 individuální a záleží na každé jednotlivé kartě či tokenu. Totéž platí i pro CSP modul

- **Microsoft Base Smart Card Crypto Provider**

který může zprostředkovávat kryptografické funkce (některých) čipových karet.

[3] Problematikou hašovací funkce SHA-2 v produktem Microsoftu se podrobněji zabývá kapitola 7.

[4] Modul CSP stejného jména (ale s příponou „(Prototype)“) se vyskytuje již v operačním systému MS Windows XP s SP3.

5.1.3.3 Programy vyžadující uživatelskou instalaci externího úložiště

Pokud si pořídíte nějaké externí úložiště na čipové kartě či USB tokenu, a v operačním systému MS Windows řádně nainstalujete jak všechny potřebné ovladače (tj. ovladače samotného zařízení či čtečky), tak i příslušný modul CSP, stále ještě nemusíte mít vyhráno. Problém je v tom, že z pohledu operačního systému je sice nové úložiště řádně nainstalováno (navázáno na rozhraní CryptoAPI), ale zdaleka ne všem aplikacím to bude stačit. Řada z nich může vyžadovat, abychom jim nové úložiště na tokenu či kartě bylo zpřístupněno individuálně takovým způsobem, jaký ony vyžadují.

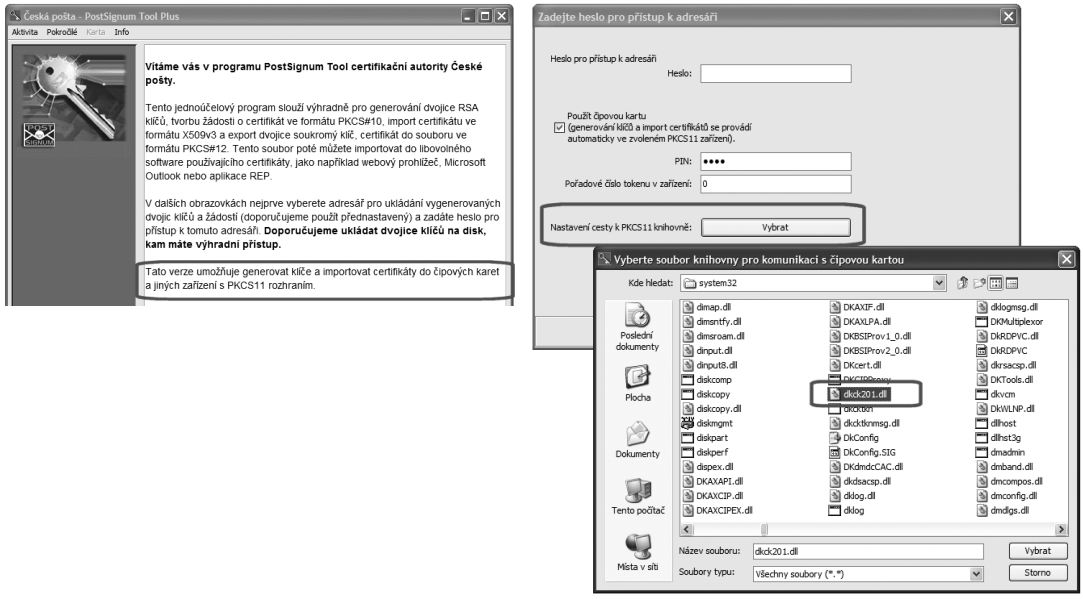
> Příkladem takových aplikací je prohlížeč Mozilla Firefox či třeba nástroj PostSignum Tool Plus, sloužící ke generování žádostí o vystavení nových certifikátů. Oba si zde ukážeme podrobněji.

Naštěstí i zde panuje určitá jednotnost: všechny tyto aplikace od nás budou chtít, abychom jim řekli, která konkrétní systémová knihovna slouží ke zpřístupnění nového úložiště a práci s ním. Takováto knihovna je obvykle označována jako **PKCS#11 modul**, resp. jako modul ve formátu PKCS#11. V prostředí MS Windows má takovýto modul formát systémové knihovny s příponou .dll.

Takovýto PKCS#11 modul najdeme nejčastěji v systémovém adresáři, kde máme umístěn operační systém Windows, a zde konkrétně v podadresáři System32. Obvykle nám ho tam zanechá instalační program, kterým jsme nechali nainstalovat kartu či token do operačního systému. Ovšem jak se tato knihovna/modul konkrétně jmenuje, je závislé na konkrétním modelu čipové karty či USB tokenu (a jméno knihovny je třeba hledat v související dokumentaci).

Obrázek 5-13

Příklad zpřístupnění USB Tokenu zadáním jeho PKCS#11 modulu

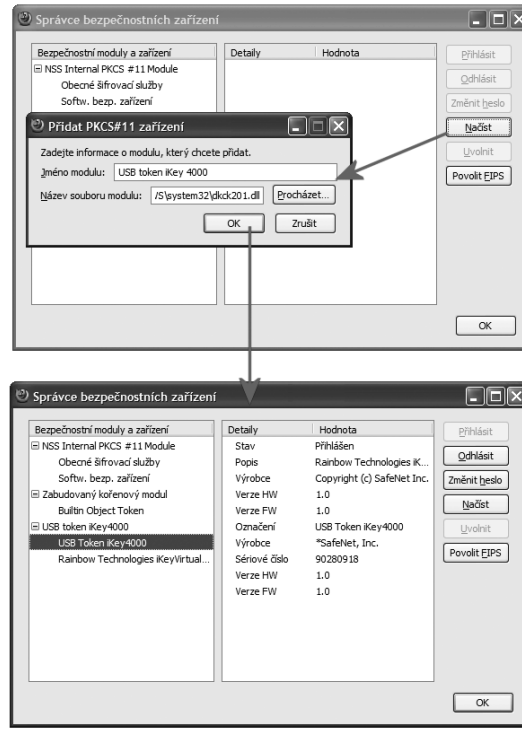


Na předchozím obrázku vidíte příklad explicitního zpřístupnění tokenu iKey4000 aplikačnímu programu PostSignum Tool Plus, který slouží pro generování žádostí o nový certifikát. Pokud chceme, aby tento program pracoval s USB tokenem, musíme mu (kromě přístupového hesla k tokenu) správně určit i příslušnou knihovnu (zde: dkck201.dll).

Pokud to neuděláme, program PostSignum Tool Plus bude schopen pracovat pouze se systémovým úložištěm operačního systému MS Windows, které je interní, realizované čistě softwarově, a pro certifikáty určené pro podepisování se příliš nehodí (důvody viz výše).

Jiným příkladem programu, kterému musíme explicitně zpřístupnit jakékoli externí úložiště, je prohlížeč Mozilla Firefox. Ten si standardně vytváří své vlastní (interní, softwarové) úložiště, které je současně (celým) jeho logickým úložištěm. Pokud chceme do tohoto logického úložiště začlenit ještě nějaké externí úložiště, a tím Firefoxu zpřístupnit certifikáty a klíče na čipové kartě či USB tokenu, musíme mu také zadat potřebnou knihovnu (PKCS#11 modul) pro zpřístupnění tohoto externího úložiště. Příklad provedení ukazuje obrázek.

Obrázek 5-14
Příklad zpřístupnění USB tokenu v prohlížeči Firefox



5.2 Příprava webového prohlížeče pro práci s elektronickými podpisy

Pracovat s elektronickým podpisem (či značkami a razítkem) můžeme prostřednictvím různých programů.

> Například pro podepisování emailových zpráv budeme nejspíše využívat náš poštovní program (například MS Outlook z balíku MS Office). Při čtení elektronicky podepsaných dokumentů ve formátu PDF zase budeme vyhodnocovat platnost podpisů a razítek přímo v programu Adobe Reader. Při podepisování vlastních elektronických dokumentů pak můžeme využívat zabudované funkce v používaném editoru či jiný nástroj, sloužící speciálně potřebám podepisování.

Velmi často ale budeme potřebovat pracovat s elektronickým podpisem, značkou či razítkem skrze náš webový prohlížeč (browser).

> Například když budeme pracovat s nějakou on-line službou (na bázi WWW), bude muset potřebné funkce podporovat právě náš prohlížeč.

Jenže mezi použitím aplikačních programů s již zabudovanou podporou kryptografie a elektronického podpisu a použitím „univerzálního“ webového prohlížeče je jeden zásadní rozdíl: pokud aplikační program (například nějaký editor, poštovní program apod.) podporuje činnosti spojené s elektronickým podpisem, je na to již dopředu vybaven. Pak stačí jen správně „naplnit“ a zpřístupnit mu to úložiště certifikátů, se kterým tento program pracuje (viz výše).

U webového prohlížeče (browseru) je tomu jinak. Prohlížeč je velmi univerzálním programem, který již z principu nemůže být dopředu připraven na všechny možné situace, ke kterým ho bude uživatel chtít využít.

Proto se u prohlížečů běžně používá strategie dodatečného instalování „toho, co je potřeba“. Tedy až v okamžiku, kdy uživatel skutečně narazí na potřebu určité funkčnosti, kterou jeho prohlížeč „sám od sebe“ (jakoby již z výroby) nepodporuje.

Praktické provedení takovéhoto rozšíření může mít více podob a může být také různě pojmenováno. Nejčastěji se hovoří o přidávání tzv. „plug-in modulů“ do prohlížečů, ale někdy může být vše prezentováno jako instalování specializované knihovny. V souvislosti s Internet Explorerem zase může jít o doplňky v podobě prvků ActiveX.

Vždy při instalaci jakýchkoli doplňků je samozřejmě třeba dbát všech zásad bezpečnosti. Minimálně kontrolovat, od koho instalovaný doplněk pochází a zda je skutečně zapotřebí.

5.2.1 XML Filler jako plug-in

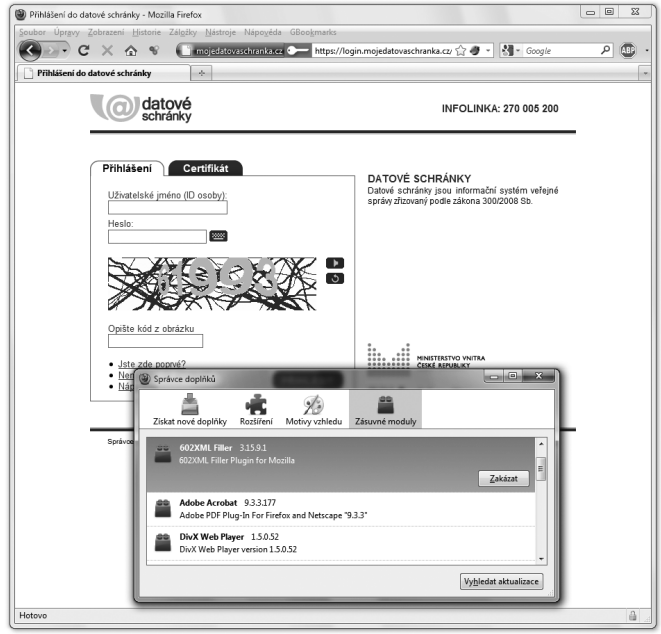
Konkrétním příkladem, který dobře znají všichni uživatelé datových schránek (přes jejich webové rozhraní), je XML Filler od společnosti Software602 (602XML Filler). Žádný prohlížeč totiž „sám od sebe“ nezná a nepodporuje specifický formát ZFO, se kterým informační systém datových schránek pracuje. Včetně toho, jak se v tomto formátu pracuje s (interními) elektronickými podpisy, značkami a časovými razítky. A tak je nutné každému prohlížeči potřebnou funkčnost dodat alespoň dodatečně, skrze příslušný modul plug-in.

Pokud vše funguje tak, jak má, je instalace potřebného plug-inu plně automatizována (alespoň pro obě nejčastěji používané varianty prohlížečů, tj. Internet Explorer a Mozilla Firefox).

Obrázek 5-15
Výzva k instalaci rozšíření pro XML Filler do Internet Exploreru

K instalaci přitom dochází v tom okamžiku, kdy prohlížeč poprvé potřebuje příslušnou funkčnost – a uživatel ji samozřejmě musí odsouhlasit.

Obrázek 5-16
Již nainstalovaný modul 602XML Filler



5.2.2 Softwarové knihovny pro podepisování

Dalším příkladem jsou softwarové knihovny, které prohlížečům dodávají schopnost pracovat s elektronickými podpisy (značkami, razítky), ale také s certifikáty a klíči v dostupných úložištích, takovým způsobem jakým to právě používaná on-line služba vyžaduje. Proto si tato služba snad vždy sama zkontroluje, zda je příslušný doplněk (realizující potřebnou softwarovou knihovnu) v prohlížeči již nainstalován. A pokud není, vyžádá si jeho nainstalování.

> Toto nainstalování může proběhnout bez vědomí uživatele, nebo s jeho explicitním souhlasem – podle toho, jaké je aktuální bezpečnostní nastavení používaného prohlížeče.

Následující obrázky ukazují dva konkrétní příklady s prohlížečem Internet Explorer a on-line službou pro generování žádosti o nový (či následný) certifikát u certifikačních autorit I.CA a PostSignum (podrobněji viz část 5.5.2). Bez instalace příslušných doplňků by prohlížeč nebyl schopen provést požadované úkony, nutné pro vytvoření žádosti o nový certifikát (což mj. zahrnuje vytvoření nových párových dat, neboli nového soukromého a veřejného klíče).

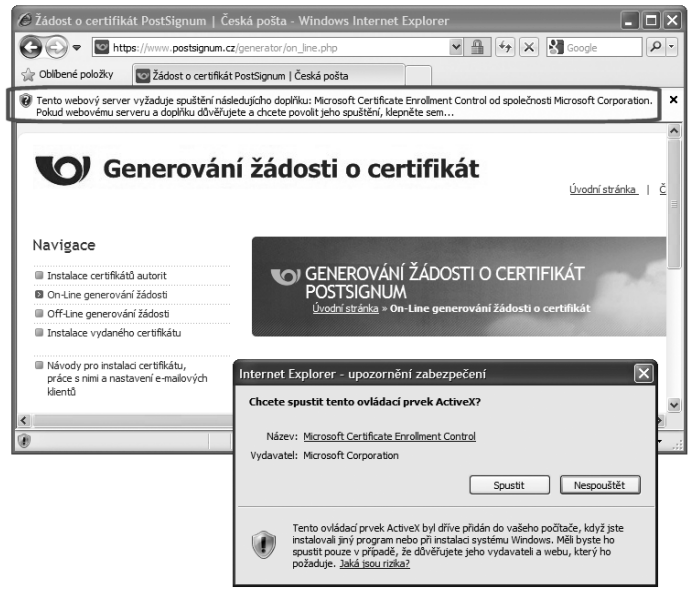
Obrázek 5-17

Příklad instalace vlastní knihovny od I.CA

Z pohledu koncového uživatele je důležité i to, že různé on-line služby mohou požadovat instalaci různých doplňků, i když tyto plní v prohlížeči obdobné či stejné úkoly. Často se totiž jedná o vlastní a specifické knihovny, bez kterých daná služba není dostupná. Takže i když si jednou nainstalujete příslušný doplněk, požadovaný jednou certifikační autoritou, je velmi pravděpodobné, že jiná certifikační autorita po vás bude chtít instalaci jiného doplňku.

Obrázek 5-18

Příklad žádosti o instalaci prvku ActiveX



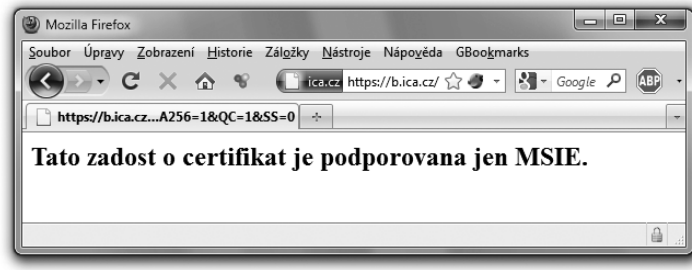
Obrázek 5-19
Příklad výzvy k instalaci knihovny CAPICOM

5.3 Formáty certifikátů

Nejrůznější knihovny, výkonné moduly či moduly plug-in, které se doinstalovávají ke konkrétním programům, mají vždy takový formát, jaký daný aplikační program vyžaduje. Tento formát je navíc závislý na konkrétní systémové platformě, na které je program provozován.

> Tato závislost na programu a platformě je mnohdy pro uživatele nepříjemná a omezující, když je nutí používat takové programy či celé systémové platformy, které běžně nepoužívají a na svých počítačích třeba ani používat nemohou. Příkladem může být řada on-line služeb, které fungují jen v Internet Exploreru na platformě MS Windows a nikde jinde.

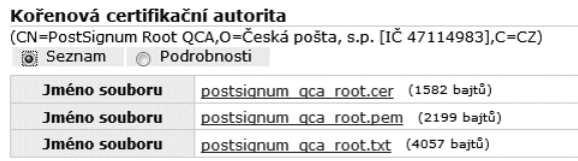
Obrázek 5-20
Příklad on-line služby (žádosti o certifikát u I. CA), která funguje jen v Internet Exploreru



Principiálně odlišná je situace u certifikátů, se kterými potřebujeme manipulovat, ať již je ukládat do úložišť certifikátů či jakkoli jinak. Zde naštěstí existují standardizované formáty, které navíc nejsou vázané na konkrétní platformu ani na používaný program.

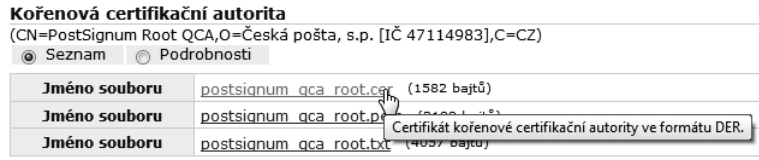
Malý příklad výčtu formátů vidíte na následujícím obrázku, který ukazuje nabídku (nového) kořenového certifikátu CA PostSignum (konkrétně PostSignum Root QCA 2).

Obrázek 5-21
Nabídka formátů kořenového certifikátu



Aby to ale nebylo tak jednoduché, první formát nabízený na obrázku je formát DER, i když je uložen v souboru s příponou .cer. To nám připomíná důležitou skutečnost: jednou věcí je formát certifikátu jako takový (definující jaká data mají být v certifikátu obsažena, jak mají být strukturována atd.).

Obrázek 5-22
Uvnitř souboru s příponou .cer je certifikát ve formátu DER



Jinou věcí pak je způsob zakódování těchto dat, a ještě jinou věcí je přípona souboru, ve kterém jsou takto zakódovaná data obsažena.

5.3.1 Standard X.509 a položky certifikátu

Pokud jde o obsah certifikátu jako takového, pak všechny certifikáty, o kterých se v této knížce zmiňujeme, vychází z mezinárodního standardu X.509 (který vydala Mezinárodní telekomunikační unie, ITU). Tento standard se přitom týká jak zde popisovaných certifikátů s veřejným klíčem, tak třeba i formátu seznamů CRL.

Standard X.509 například definuje to, jaké konkrétní položky má každý certifikát obsahovat. Ukažme si to na malém (a neúplném) příkladu, i s obsahem položek konkrétního osobního certifikátu:

Jméno položky	Český překlad jména položky[5]	Význam položky	Příklad hodnoty
Version	Verze	verze standardu X.509	3
Serial Number	Sériové číslo	sériové číslo certifikátu u jeho vydavatele	261802
Signature algorithm	Algoritmus podpisu	jaký algoritmus má být použit pro el. podpis	Sha256RSA
Issuer	Vystavitel	jméno certifikační autority, která certifikát vystavila	CN=PostSignum Qualified CA,O=Česká pošta, s.p. [IČ 47114983],C=CZ
Valid not	Platnost od	od jakého okamžiku začíná řádná platnost certifikátu	Fri Jan 15 10:18:48 CET 2010
Valid not after	Platnost do	k jakému okamžiku končí řádná platnost certifikátu	Sat Jan 15 09:28:00 CET 2011
Subject	Předmět (subjekt certifikátu)	komu byl certifikát vystaven	SerialNumber=P135491, CN=RNDr. Ing. Jiří Peterka, OU=P135491,C=CZ
Certificate Policies	Zásady certifikátu	další informace o certifikátu a jeho statutu	displayText: Tento kvalifikovany certifikat byl vydan podle zakona 227/2000Sb. a navaznych predpisu./This qualified certificate was issued according to Law No 227/2000Coll. and related regulations
CRLDistribution Points	Distribuční místa seznamu odvolaných certifikátů	URL místa, kde lze nalézt seznam odvolaných (revokovaných) certifikátů)	URL=http://www.postsignum.cz/crl/psqualifiedca.crl
KeyUsage	Použití klíče	K jakým účelům lze použít klíče, ke kterým se certifikát vztahuje	digitalSignature | nonRepudiation | keyEncipherment

Každý certifikát, vycházející ze standardu X.509, tedy obsahuje řadu zajímavých údajů. Samozřejmě zde najdeme takové údaje, jako kdy začíná a kdy končí řádná platnost certifikátu (položky Valid not before, not after).

Již zde ale nenajdeme informaci o tom, že daný certifikát byl odvolán, a že jeho řádná platnost tudíž skončila předčasně. Důvody jsme si popsali v části 3.4, kde jsme si také uvedli, že informaci o případné revokaci je třeba hledat u vydavatele certifikátu (certifikační autority). Kde konkrétně, udává položka CRLDistributionPoints.

[5] Nejde o oficiální překlad, ale o překlad používaný v českých verzích operačního systému MS Windows.

Velmi důležité jsou i položky, které popisují druh certifikátu: v předchozím příkladu je v položce „Certificate Policies“ explicitně uvedeno, že se jedná o kvalifikovaný certifikát (a tím o osobní kvalifikovaný certifikát). V případě kvalifikovaného systémového certifikátu bychom ve stejné položce našli explicitní konstatování, že jde o kvalifikovaný systémový certifikát. Připomeňme si ale, že naopak to neplatí: pokud nějaký certifikát není kvalifikovaný, nenajdeme v něm žádnou explicitní informaci typu „tento certifikát není kvalifikovaný“.

S typem certifikátu souvisí i vymezení toho, k čemu je možné certifikát využít. Přesněji: k čemu je možné využít soukromý klíč, ke kterému se certifikát vztahuje (viz část 4.3.1). To vyjadřuje položka „KeyUsage“.

Velmi důležitým údajem je také údaj o vystaviteli certifikátu (Issuer): zde je uvedeno jméno příslušné certifikační autority. Právě tento údaj je pro nás vodítkem k posuzování důvěryhodnosti certifikátu. Závazné jsou nicméně jiné položky (viz část 3.5.2).

A snad nejdůležitější je položka „Subject“ (v české lokalizaci buď Subjekt, nebo Předmět), která vypovídá o tom, komu byl certifikát vystaven, resp. kdo je jeho držitel. Tím pádem i o tom, kdo je podepsanou osobou (pokud hodnotíme něčí podpis, založený na daném certifikátu).

5.3.1.1 DN: Distinguished Name

Obě posledně jmenované položky (Issuer a Subject, pro vydavatele a držitele certifikátu) tedy identifikují určitý subjekt, ať již v roli vydavatele certifikátu (Issuer) či v roli jeho držitele (Subject).

Jméno příslušného subjektu, které je v jedné či druhé položce uvedeno, se vyjadřuje pomocí řetězce **Distinguished Name** (zkratkou DN). Tento řetězec, se kterým jsme se seznámili již v části 4.9.1, je tvořen několika dílčími složkami, z nichž každá je uvozena jedno či dvoupísmennou zkratkou, která určuje význam celé složky. Zde je několik nejčastěji používaných složek:

- **CN** (Common Name) : jméno držitele, resp. certifikační autority (jako vydavatele)
- **O** (Organization): organizace, jejímž je držitel či vydavatel certifikátu členem
- **OU** (Organizational Unit): obdobně, pro organizační složku
- **C** (Country): země
- **L** (Locality): adresa
- **E** (email): emailová adresa
- **T** (Title): titul, pracovní zařazení fyzické osoby (držitele certifikátu)

Rozsah ani konkrétní výčet dílčích složek, které dohromady tvoří jméno DN (Distinguished Name), není předepsáno a může se v praxi lišit. Povinná je pouze složka CN (Common Name). Navíc na pořadí, v jakém jsou jednotlivé dílčí složky v rámci DN uváděny, nezáleží.

V případě certifikačních autorit obvykle není s řetězcem DN problém, protože používaná skladba dílčích složek obvykle stačí k jednoznačné identifikaci konkrétní certifikační autority. Ukázku konkrétních hodnot jmen DN pro jednotlivé certifikační autority PostSignum ukazuje následující tabulka.

Certifikační autorita	DN (Distinguished Name)
(původní) kořenová certifikační autorita PostSignum	CN=PostSignum Root QCA, O=Česká pošta, s.p. [IČ 47114983], C=CZ
podřízená kvalifikovaná certifikační autorita PostSignum	CN=PostSignum Qualified CA, O=Česká pošta, s.p. [IČ 47114983],C=CZ
podřízená veřejná certifikační autorita PostSignum	CN=PostSignum Public CA, O=Česká pošta, s.p. [IČ 47114983],C=CZ
„nová“ (dvojková) kořenová certifikační autorita PostSignum	CN=PostSignum Root QCA 2, O=Česká pošta, s.p. [IČ 47114983], C=CZ
„nová“ (dvojková) podřízená kvalifikovaná certifikační autorita PostSignum	CN=PostSignum Qualified CA 2, O=Česká pošta, s.p. [IČ 47114983],C=CZ
„nová“ (dvojková) podřízená komerční certifikační autorita PostSignum	CN=PostSignum Public CA 2, O=Česká pošta, s.p. [IČ 47114983],C=CZ

Problém v praxi může vznikat spíše s jednoznačnou identifikací držitele certifikátu, v případě že jde o fyzickou osobu bez vazby na zaměstnavatele. U zaměstnaneckých certifikátů pomáhá právě údaj o zaměstnavateli, případně o pracovní pozici, obsažený ve jméně DN. Někdy může jít skutečně o velmi detailní údaje, jako například:

> SERIALNUMBER=QCA-4542, T=referent živnostenského rejstříku (m324), EMAILADDRESS=-klara.novakova@cityofprague.cz, CN=Klára Nováková, OU=oddělení sekretariátu a živnostenského rejstříku, OU=Odbor živnostenský a občanskoprávní, OU=Magistrát hlavního města Prahy, O=Hlavní město Praha, C=CZ

Ale u osobních certifikátů, které nejsou zaměstnanecké, a navíc třeba s emailovou adresou na nějakém freemailu, již může být jednoznačná identifikace držitele certifikátu skutečně problematická. Až nemožná. Schválně, kterému Janu Krausovi patří certifikát, který vystavila jako kvalifikovaný společnost eIdentity, s následujícím řetězcem DN:

> SERIALNUMBER=QCA-2548, EMAILADDRESS=jan.kraus@gmail.com, CN=Jan Kraus, OU=Clients, O=eIdentity a.s., C=CZ

Připomeňme si v této souvislosti důležitou skutečnost, o které jsme se zmiňovali již v předchozí kapitole: že certifikační autority, které vydávají kvalifikované certifikáty, mají velmi detailní informace o identitě každé fyzické osoby, které certifikát vystaví. Tyto informace si ale z větší části ponechávají pro sebe, zatímco do samotných certifikátů (které jsou veřejné) z nich dávají jen část.[6]

Někdy je jediným relevantním údajem pouze položka CN (Common Name) se jménem a příjmením, jako ve výše uvedeném příkladu. Také emailová adresa na freemailu, kterou si každý může pojmeno-

[6] Zbývající informace o identitě držitele certifikátu, které certifikační autorita má k dispozici, již nejsou veřejně dostupné. Možnost jejich získání mají kupř. orgány činné v trestním řízení, ale běžný uživatel nikoli.

vat, jak chce, nám moc nepomůže. Teoreticky by mohlo pomoci „rozlišovací jméno“ (se sériovým číslem držitele certifikátu). Jenže to se vztahuje k interní evidenci klientů certifikační autority a širší uživatelské veřejnosti příliš nepomůže.

5.3.1.2 Formáty DER a PEM (pro certifikáty)

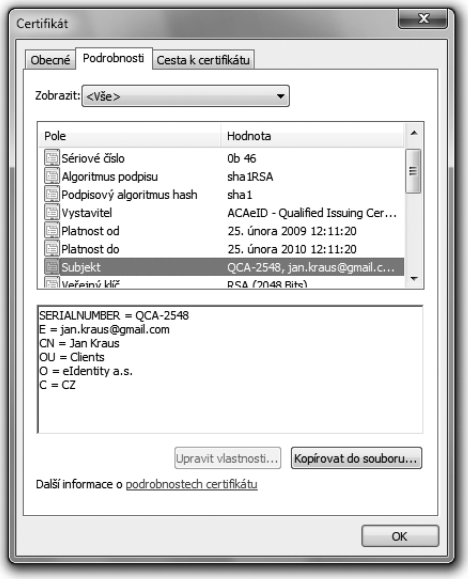
Pokud jde o kódování těch dat, která tvoří certifikát (dle X.509), pak i zde existuje více možností. Jednou z nich je binární kódování, jakým je například již zmiňované kódování **DER (Distinguished Encoding Rules).** Současně jde i o formát, protože definuje, jak mají být takto zakódovaná data zapsána do nějakého souboru.

Příklad si zde nemůžeme vypsat, jelikož jde o binární data. Pro programy je ale DER, jako binární tvar, dobře srozumitelný. A tak si můžeme ukázat alespoň to, jak certifikáty v tomto kódování a formátu zobrazuje nějaký program, konkrétně systémová utilita v operačním systému MS Windows.

Jde ostatně o zobrazení certifikátu, které jsme si již několikrát ukazovali.

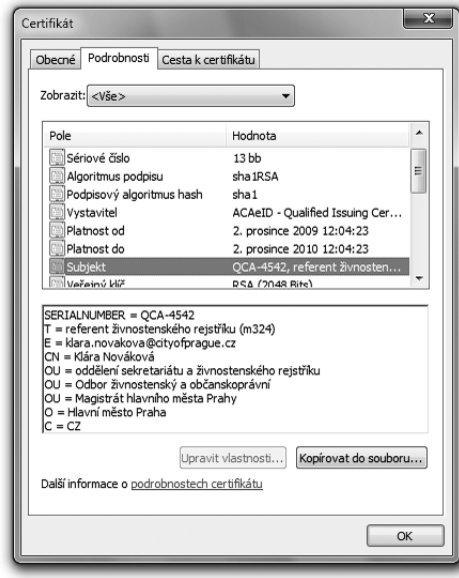
Obrázek 5-23

Příklad certifikátu s málo podrobným jménem DN



Obrázek 5-24

Příklad certifikátu s velmi podrobným jménem DN



Pokud bychom chtěli nějak vypsat data, tvořící certifikát, mohli bychom je nejprve převést do tisknutelné, a tedy již nikoli binární podoby. Jednou z možností, jak to udělat, je využít (obecné) kódování Base64, známé z elektronické pošty.[7]

Pokud to uděláme, a data v kódování Base64 prefixujeme řádkem

-----BEGIN CERTIFICATE-----

a zakončíme řádkem

-----END CERTIFICATE-----

můžeme hovořit o formátu **PEM** (od: Privacy Enhanced Mail). Příklad kořenového certifikátu CA Post-Signum QCA ve formátu PEM ukazuje obrázek.

Pro člověka asi nejpřehlednější možností, jak si vypsat data obsažená v certifikátu, je čistě textová forma. Příklad (byť jen s úryvkem textové podoby konkrétního certifikátu) vidíte na následujícím obrázku:

---

[7] Přesněji ze standardu MIME pro elektronickou poštu.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 100 (0x64)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Root QCA 2
        Validity
            Not Before: Jan 19 08:04:31 2010 GMT
            Not After : Jan 19 08:04:31 2025 GMT
        Subject: C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Root QCA 2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a0:5c:fc:c8:1c:5f:da:07:f5:b8:dd:06:19:79:
                    27:bc:61:f0:ba:ba:69:e0:bc:37:64:f5:99:07:a9:
                    c4:04:31:a3:48:62:17:2b:43:ab:e9:76:b7:65:3f:
                    ad:54:34:de:51:48:d3:d7:7d:c6:ed:5b:39:d4:3e:
                    b3:fd:28:56:cb:ef:53:ed:ad:5f:e9:72:27:6a:47:
                    b0:c8:58:fc:3d:3d:04:75:9e:2d:03:26:cd:61:d1:
                    14:3b:f7:52:86:0d:96:bd:4c:9f:65:f5:c7:d2:39:
                    a6:66:6e:aa:50:3c:b4:55:f2:90:7e:2c:96:72:14:
                    11:8b:f0:31:eb:35:da:53:6f:97:de:15:c1:7e:f4:
                    4c:af:99:7a:ce:0c:58:54:04:c4:cb:10:9f:38:b3:
                    3d:6b:95:3a:96:1a:72:08:37:f6:1a:0e:9d:3d:ce:
                    42:cb:a4:30:60:61:a9:60:44:75:7f:32:c6:b0:df:
                    6c:b5:db:ad:93:09:4f:d7:70:c7:53:54:a9:e9:6e:
                    72:c2:d7:cb:a3:06:1a:57:56:ea:38:e7:40:45:b0:
                    28:27:ba:bc:2c:ee:84:06:3c:88:56:bd:37:98:5b:
                    ac:3d:a3:02:3b:37:04:9f:7c:cb:e5:76:9f:92:73:
                    37:e9:5a:ad:76:6a:b3:89:64:7e:dd:44:40:52:0a:
                    84:d3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:
                URI:http://www.postsignum.cz/crl/psrootqca2.crl
                URI:http://www2.postsignum.cz/crl/psrootqca2.crl
                URI:http://postsignum.ttc.cz/crl/psrootqca2.crl

            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy (OID 2.5.29.32.0)

                  User Notice:
                    Explicit Text: Tento kvalifikovany systemovy certifikat byl vydan podle
zakona 227/2000Sb. a navaznych predpisu/This qualified system certificate was issued accor-
ding to Law No 227/2000Coll. and related regulations
```

5.3.2 Standardy PKCS

V běžné praxi elektronického podpisu je nutné řešit i další aspekty, než jen strukturu certifikátů (což dělá standard X.509) a způsob kódování jejich obsahu (např. DER či PEM). Třeba formát podepsaných dokumentů či datových zpráv, nebo jen formát (externích) podpisů, značek a časových razítek. Stejně tak formát certifikátů, ať již samotných či v jednom celku s odpovídajícím soukromým klíčem, nebo formát žádostí o vydání nového certifikátu a další náležitosti.

I zde jsou zapotřebí standardy, které by řekly, jak takovéto věci dělat. Jak reprezentovat různé objekty (hlavně podpisy, certifikáty a klíče) a jak je „dávat dohromady“ jednotným způsobem, který by všichni znali a všichni mu rozuměli stejně.

V praxi jsou pro tyto účely nejčastěji využívány standardy, označované společně jako PKCS (od: Public Key Cryptography Standards). V překladu: Standardy kryptografie s veřejným klíčem.

Vytvořila je jedna konkrétní komerční firma (RSA Security), ale staly se otevřeným a univerzálně používanými standardy. Jde přitom o celou rodinu dílčích standardů, které pokrývají řadu různých aspektů a jsou kvůli tomu uspořádány do disjunktních „řad“. Ty jsou odlišeny pomocí číslování. Tedy číslem, které následuje za zkratkou PKCS po znaku „#“.

Z našeho pohledu jsou zajímavé řady:

- **PKCS#7:** týká se formátu (podepisovaných či šifrovaných) zpráv, certifikátů či samostatných (externích) podpisů
- **PKCS#10:** řeší formát žádosti o vydání certifikátu (který se předává certifikační autoritě)
- **PKCS#11:** definuje rozhraní API k výměnným úložištím certifikátů (USB tokenům či čipovým kartám), viz část PKCS#11: definuje rozhraní API k výměnným úložištím certifikátů (USB tokenům či čipovým kartám), viz část 5.1.3
- **PKCS#12:** řeší společné ukládání certifikátů a soukromých klíčů (jak "dát dohromady" veřejný certifikát a soukromý klíč)

5.3.2.1 Formát PKCS#7 (pro podpisy i certifikáty)

Pokud pracujeme s certifikáty, které jsou strukturovány podle standardu X.509 (což jsou všechny certifikáty, uvažované v této knize), je další možností pro kódování a formátování jejich obsahu – vedle PEM, DER a čistě textové podoby – také využití standardů PKCS řady 7 (PKCS#7).

Certifikát, který je kódován a formátován dle PKCS#7, je kompatibilní s formátem PEM. Oba tvary (dle PKCS#7 a PEM) lze dokonce mezi sebou snadno převádět, aniž by přitom bylo třeba provádět nějakou kryptografickou operaci (například něco šifrovat či dešifrovat).

Obsah certifikátu, který je kódován podle PKCS#7, poznáme snadno podle toho, že je uvozen a zakončen pomocí řetězců **-----BEGIN PKCS7-----** a **-----END PKCS7-----** .

Formát PKCS#7 je ale možné (a asi i vhodnější) si představovat spíše jako určitý kontejner, do kterého lze uložit i jiné objekty, než jsou samotné certifikáty. Je možné do něj vkládat i elektronické podpisy jako takové (či elektronické značky nebo časová razítka) či třeba seznamy CRL. Stejně tak dokáže pojmout i celé datové zprávy (či dokumenty) včetně jejich podpisů. Tedy jakoby „dát dohromady" samotný dokument i s jeho podpisem.

5.3.2.2 Kódování PKCS#12 (pro certifikáty a soukromé klíče)

V některých situacích, jako například při „přenosu" soukromého klíče z jednoho úložiště do druhého (exportu z původního a importu do druhého), potřebujeme „dát dohromady" soukromý klíč s certifikátem, který se k soukromému klíči vztahuje. A to takovým způsobem, aby vznikl jeden celek, se kterým se pak dá (jako s jedním celkem) také manipulovat.

Spojení soukromého klíče a (veřejného) certifikátu je ale přeci jen náročnější, než pouhé „zapouzdření" do společného obalu (kontejneru), jaké realizuje formát PKCS#7. Jeho úloha je snazší v tom, že nakládá s objekty, které jsou považovány za veřejné – a tak nemusí zajišťovat jejich důvěrnost.

Naproti tomu soukromý klíč je soukromým právě proto, že by měl být maximálně chráněn, tak aby se nedostal do rukou nikomu nepovolanému. Takže i když ho budeme chtít „zabalit“ do jednoho společného celku s veřejným certifikátem, stále ho budeme muset chránit před neoprávněným přístupem. Tedy vhodně zašifrovat a umožnit přístup k němu jen po zadání správného hesla.

To vše má na starosti formát PKCS#12, který se pro tento účel používá.

5.3.3 Přípony souborů s certifikáty (a klíči)

Připomeňme si znovu, že formát (a kódování) certifikátu, ať již samotného, či spolu se soukromým klíčem, je věc jedna, a přípona souboru věc druhá.[8]

Asi nejlépe to lze dokumentovat na skutečnosti, že pro jeden formát se mohou používat různé přípony souborů, které se navíc mohou lišit i podle systémové platformy. Tak například „samotný“ certifikát vám někdo může dát v souboru, který má (na platformě MS Windows) příponu .cer, .crt, ale třeba také .spc či .p7b.

> Například certifikační autorita PostSignum vydává své kvalifikované certifikáty zákazníkům obvykle v souborech s příponou.crt. Certifikační autority I. CA a eIdentity zase většinou v souborech s příponou .cer.

Ještě další přípony se pak používají v případě, kdy soubor obsahuje něco ještě jiného, než je certifikát a/nebo soukromý klíč. Jako například když jde o CRL seznam či o časové razítko.

> Jedním z výčtů často používaných přípon souborů s certifikáty, podpisy, značkami či razítky je ten, který připouští datové schránky. Na informačním webu o datových schránkách je ale tento výčet (chybně) prezentován jako výčet formátů, i když ve skutečnosti jde o přípony souborů:

- CER, CRT, DER, PK7 – formáty certifikátů dle standardu X.509
- P7B, P7C, P7F, P7M, P7S – formáty certifikátů a elektronických podpisů dle PKCS#7
- TST – formát pro elektronické razítko

Nejčastěji používané kombinace formátů a přípon souborů (obvyklých na platformě MS Windows) ukazuje následující tabulka.

---

[8] Nejpřesnější by bylo mluvit zde o tzv. MIME typu: například certifikát ve formátu PKCS#7 má MIME typ ***application/xx509-ca-cert****, a ten musí být asociován s konkrétní příponou (například .cer, .crt).*

	Dle standardu	Formát	Přípony souboru
žádost o certifikát	PKCS	PKCS#10	.req, .p10
certifikát	X.509	DER	.der, .cer, .crt
		PEM	.pem
	PKCS	PKCS#7	.p7b, p7c, pk7, .spc
certifikát a soukromý klíč	PKCS	PKCS#12	.pfx, .p12
CRL seznam	PKCS	PKCS#7	.crl
žádost o časové razítko	PKCS	PKCS#7	.tsq
(již vytvořené) časové razítko	PKCS	PKCS#7	.tst

5.4 Správa certifikátů třetích stran

Jak jsme si již dříve popisovali, ke správnému fungování všech programů, které nám zprostředkovávají práci s elektronickými podpisy, značkami a časovými razítky, je nutné jim přesně vymezit, kterým certifikátům mají důvěřovat. Tedy které certifikáty mají považovat je za důvěryhodné.

Jak již víme, toto vyjádření provedeme uložením (nainstalováním) příslušných certifikátů do toho úložiště (důvěryhodných) certifikátů, které daný program používá. Konkrétní postup je přitom mírně odlišný podle toho, zda jde o certifikáty naše vlastní, nebo zda jde o certifikáty třetích stran. Připomeňme si hlavní rozdíl mezi oběma variantami:

- k vlastním certifikátům máme i odpovídající soukromé klíče a nakládáme s nimi společně. Proto bychom měli pečlivě vážit, v jakém úložišti si takovéto dvojice (certifikát+klíč) budeme uchovávat. Nejlépe v nějakém externím úložišti na čipové kartě či USB tokenu.
- k certifikátům třetích stran nemáme (a ani nemůžeme mít) odpovídající soukromé klíče. Jsou to totiž buď certifikáty jiných uživatelů, nebo certifikáty certifikačních autorit. Ale jelikož jsou tyto certifikáty plně veřejné, můžeme je bez obav uchovávat i v interních (čistě softwarových) úložištích.

Zde se podrobněji zastavíme u správy certifikátů třetích stran. Správu vlastních certifikátů (a soukromých klíčů) si necháme do závěrečné části této kapitoly, kde se budeme věnovat i generování žádostí o vydání certifikátu.

5.4.1 Není úložiště jako úložiště

Než se pustíme do konkrétnějších postupů, připomeňme si (či nově naznačme) základní skutečnosti kolem úložišť certifikátů, o kterých bychom měli vědět.

Připomeňme si již několikráte zdůrazněnou skutečnost, že každý program obecně má a používá své vlastní (logické) úložiště certifikátů. A právě – a pouze – tomuto úložišti důvěřuje v tom smyslu, že v něm uložené certifikáty považuje za důvěryhodné.

Počítejme proto s tím, že každému programu, který chceme používat pro práci s elektronickými podpisy, musíme znovu a explicitně určovat, čemu má důvěřovat (skrze instalování příslušných certifikátů do jeho úložiště). A berme jako příjemnou výjimku z tohoto pravidla, když nějaké programy dokáží sdílet jedno společné úložiště.

> Připomeňme si, že v prostředí MS Windows existuje jedno „systémové" úložiště certifikátů, realizované jako interní (a čistě softwarovými prostředky) na úrovni operačního systému jako takového. Toto úložiště používají (a tudíž sdílejí) aplikační programy od Microsoftu. Tedy jak prohlížeč Internet Explorer, tak třeba MS Outlook, MS Word a další součásti balíku MS Office.
>
> Naproti tomu prohlížeč Mozilla Firefox používá vlastní úložiště a není schopen přejít na používání systémového úložiště v MS Windows.
>
> Program Adobe Reader také má vlastní úložiště certifikátů, ale na vyžádání je schopen pracovat se systémovým úložištěm v MS Windows.

Pamatovat bychom měli i na to, že snad všechna interní úložiště certifikátů, která si pro své potřeby vytváří konkrétní programy – včetně toho systémového – jsou již „od výrobce" nějak zabydlena, resp. naplněna určitými certifikáty. Tvůrce programu tak vlastně za nás dopředu vyjádřil důvěru některým certifikačním autoritám (skrze jejich certifikáty) – což nám jako uživatelům může výrazně usnadnit život. Ale také nám ho může zkomplikovat, pokud o tom nevíme. Případně když s hodnocením producenta programu nesouhlasíme (a neprosadíme si svou vůli přes vůli tvůrce programu).

5.4.2 Struktura úložišť certifikátů

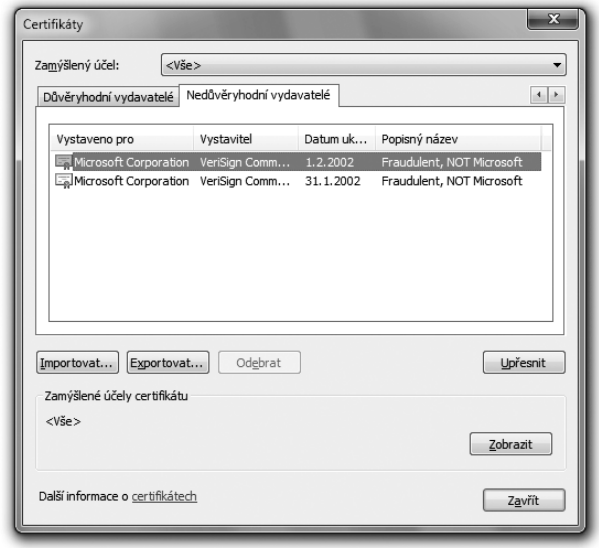
Na interních úložištích certifikátů je zajímavé i to, že jsou často různě strukturovaná. Toto jejich strukturování se projevuje existencí více různých složek, do kterých lze umisťovat (vlastně: třídit) jednotlivé certifikáty.

Až na jednu výjimku (viz dále) přitom platí, že umístěním konkrétního certifikátu do kterékoli složky dochází k vyjádření důvěry tomuto certifikátu – a program, který s úložištěm pracuje, bude tento certifikát považovat za důvěryhodný.

> Onou výjimkou je složka pro certifikáty od nedůvěryhodných vydavatelů v systémovém úložišti v MS Windows: umístěním certifikátu do této složky se naopak explicitně vyjadřuje nedůvěra příslušnému certifikátu. Efekt je stejný, jako kdyby byl příslušný certifikát revokován.

Důvodem pro existenci více složek v rámci jednoho úložiště je zřejmě také větší přehlednost. Při větším počtu certifikátů je toto členění v podstatě nutností pro „udržení pořádku". Při malém počtu certifikátů v úložišti se naopak může jevit jako zbytečné. Nicméně existence různých složek často přináší i určitou přidanou hodnotu: zařazením konkrétního certifikátu do konkrétní složky můžeme vyjádřit určitou informaci o tomto certifikátu, a ta pak může být využita pro efektivnější práci s ním.

Obrázek 5-25
Obsah složky pro nedůvěryhodné certifikáty v systémovém úložišti MS Windows



Tak například: jedna ze složek bývá tradičně vyhrazena pro osobní certifikáty aktuálního uživatele. Právě (a pouze) do této složky se pak umisťují osobní certifikáty i se soukromým klíčem, a právě a pouze do této složky se „promítají“ osobní certifikáty i se soukromými klíči, uložené na čipové kartě či USB tokenu.

Nebo: (nejméně) jedna ze složek bývá vyhrazena pro certifikáty certifikačních autorit. To usnadňuje vyhledávání certifikačních cest (posloupností certifikátů, vedoucí od daného k nějakému kořenovému certifikátu certifikační autority. A dokonce to umožňuje automatické přidávání „dceřiných“ certifikátů certifikačních autorit, které si budeme popisovat později.

Na druhou stranu může být takovéto vnitřní strukturování úložišť certifikátů i zdrojem nepříjemných chyb. Pokud totiž uložíme (nainstaluje určitý certifikát) do nesprávné složky, může to mít úplně jiný význam oproti tomu, kdybychom jej nainstalovali do správné složky.

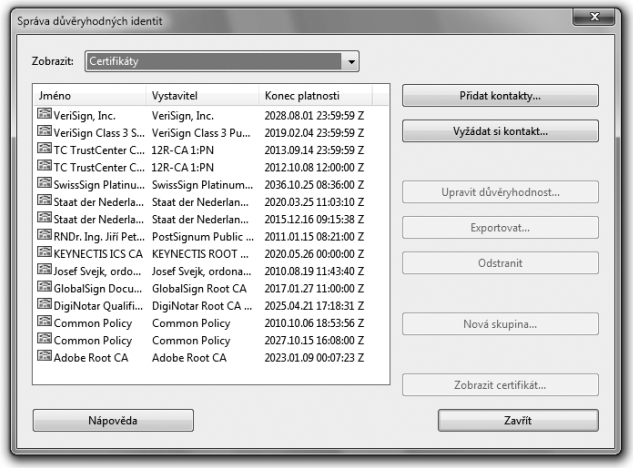
5.4.2.1 Úložiště certifikátů programu Adobe Reader

Příkladem nejjednoduššího úložiště certifikátů je to, které používá program Adobe Reader. Tedy pokud tento program není nastaven tak, aby současně využíval i systémové úložiště certifikátů operačního systému MS Windows.

Toto vlastní interní úložiště Adobe Readeru není nijak strukturováno. Nemá tedy žádné složky, a všechny certifikáty zde jsou umístěny „na jedné hromadě“. Pro malý počet certifikátů to je únosné řešení – a v případě Adobe Readeru koreluje s tím, že při instalaci Readeru je do tohoto úložiště vloženo (instalováno) jen několik málo certifikátů (jako jeho „počáteční výbava“).

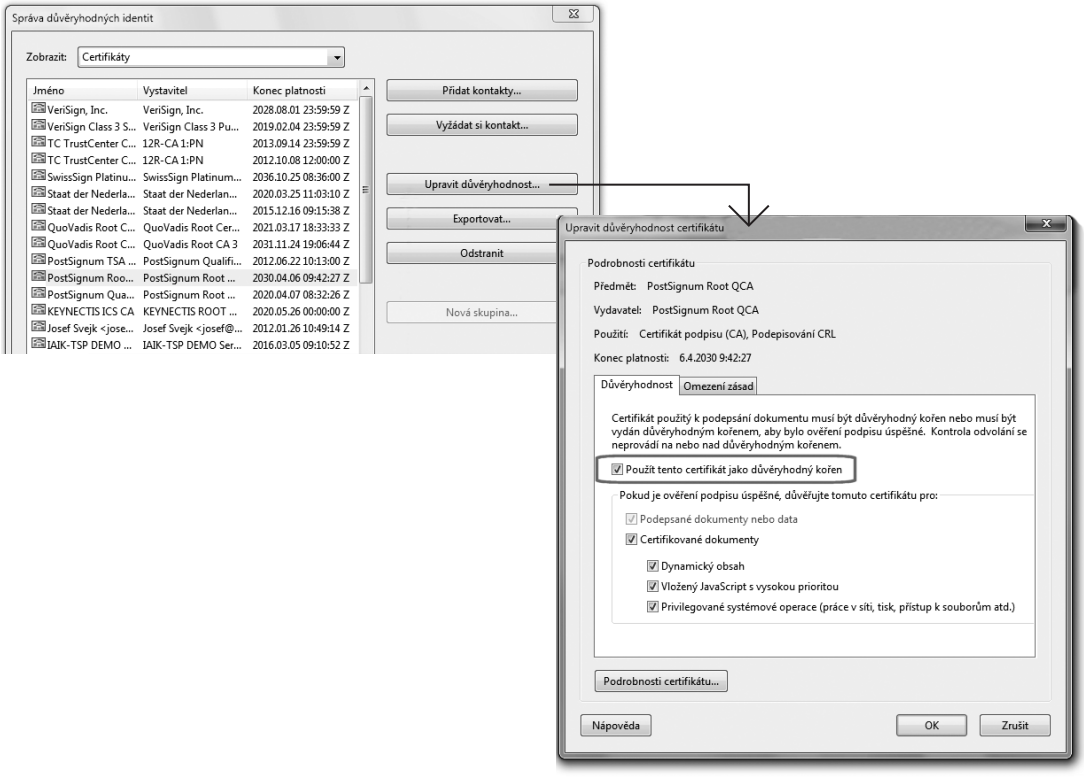
Obrázek 5-26

Úložiště certifikátů programu Adobe Reader



Obrázek 5-27

Certifikát v úložišti v úložišti Adobe Readeru je označen za kořenový



Na druhou stranu i toto úložiště přeci jen má určité členění, protože musí alespoň nějak rozlišovat mezi certifikáty, které jsou v něm obsaženy. Minimálně totiž potřebuje vědět, které z certifikátů jsou kořenové (a nezkoumal u nich případnou revokaci). A to mu musí říci uživatel, skrze „úpravu důvěryhodnosti" certifikátu. Příklad, s kořenovým certifikátem PostSignum, vidíte na předchozím obrázku (viz obrázek 5-27).

I přes svou jednoduchost ale má úložiště certifikátů programu Adobe Reader schopnost pracovat s externími úložišti a se soukromými klíči a vlastními certifikáty svého uživatele. Souvisí to s tím, že i Adobe Reader má určité schopnosti pro vytváření elektronických podpisů, které si budeme podrobněji popisovat v kapitole 6. Zde si také ukážeme, jak konkrétně nastavit vlastní úložiště Readeru, aby dokázalo pracovat s externím úložištěm (například na USB tokenu nebo čipové kartě).

Jak si také řekneme později (v částech 5.4.3 a 5.4.4), i toto úložiště je při instalaci Adobe Readeru vybaveno určitou „počáteční náplní", která může být postupně rozšiřována automatickým dočítáním dalších kořenových certifikátů certifikačních autorit, stahovaných ze serverů společnosti Adobe.

5.4.2.2 Úložiště certifikátů prohlížeče Mozilla Firefox

Příkladem „středně složitého" úložiště certifikátů může být to, které používá prohlížeč Mozilla Firefox. A to vždy a bez výjimky, protože Firefox neumí (alternativně) používat systémové úložiště certifikátů v operačním systému MS Windows, jako to umí Adobe Reader. Umí ale pracovat s externími úložišti, byť vyžaduje jejich explicitní připojení (postupem, naznačeným v části 5.1.3).

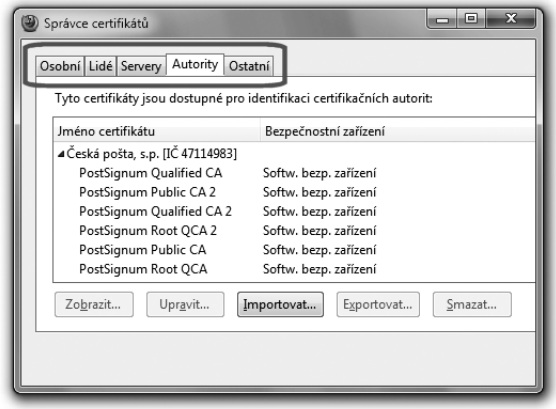
Úložiště Firefoxu je členěno na následující složky:

- **Osobní:** pro osobní certifikáty aktuálního uživatele
- **Lidé:** pro osobní certifikáty ostatních osob
- **Servery:** pro systémové (serverové) certifikáty, přidělované konkrétním serverům
- **Autority:** pro certifikáty certifikačních autorit, a to jak kořenových tak i podřízených (zprostředkujících)
- **Ostatní**

Do všech těchto složek (s výjimkou složky „ostatní") lze instalovat nové certifikáty: do složky „Osobní" včetně soukromých klíčů,[9] do ostatních složek jen samotné certifikáty. Obsah případného externího úložiště s vlastními certifikáty a soukromými klíči (na čipové kartě či tokenu) se „promítá" také do složky „Osobní".

K certifikátům, umístěným ve složce „Autority", mohou být automaticky „dočítány" jejich podřízené certifikáty (viz dále).

Obrázek 5-28
Vnitřní struktura úložiště prohlížeče Firefox

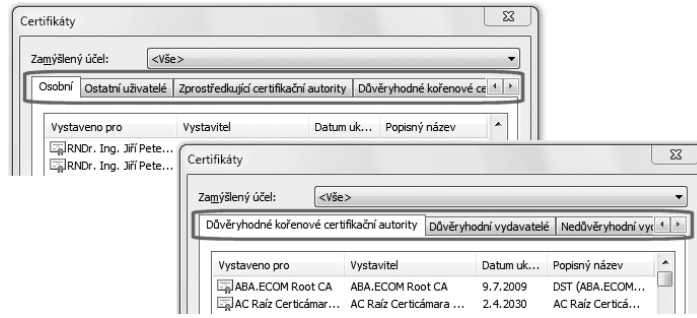


Při instalaci konkrétních certifikátů do úložiště Firefoxu je plně na uživateli, aby zvolil složku, do které má být certifikát vložen. K této volbě je uživatel donucen tím, že každá složka má svůj vlastní mechanismus („tlačítko“) pro vkládání, resp. import. Nejprve je tedy třeba zvolit složku, a teprve do ní pak lze instalovat (vkládat, importovat) certifikát, skrze příslušnou volbu („importovat“).

5.4.2.3 Systémové úložiště certifikátů v MS Windows

Nejvíce strukturované je systémové úložiště certifikátů v operačním systému MS Windows. To je standardně tvořeno interním úložištěm, které je realizováno čistě softwarovými prostředky. Ale i k němu lze „připojit“ externí úložiště, jehož obsah se do systémového úložiště vhodně promítne.

Obrázek 5-29
Složky systémového úložiště MS Windows



[9] Ve formátu PKCS#12.

Systémové úložiště MS Windows má řadu „složek“ pro různé významy certifikátů:

- **Osobní:** pro certifikáty aktuálního uživatele
- **Ostatní uživatelé:** pro osobní certifikáty jiných fyzických osob
- **Zprostředkující certifikační autority** (viz dále)
- **Důvěryhodné kořenové certifikační autority**
- **Důvěryhodní vydavatelé**
- **Nedůvěryhodní vydavatelé**

Poměrně specifický význam má složka „Nedůvěryhodní vydavatelé“, zmiňovaná již dříve: umístěním konkrétního certifikátu do této složky se mu vyjadřuje nedůvěra, ve stejném smyslu jako kdyby tento certifikát byl revokován (k okamžiku začátku své platnosti).

Význam složky „Osobní“ je u tohoto systémového úložiště stejný, jako v případě úložiště prohlížeče Firefox: sem se instalují osobní certifikáty i se soukromými klíči, a sem se také „promítají“ vlastní certifikáty a soukromé klíče z případného externího úložiště (na čipové kartě či na USB tokenu).

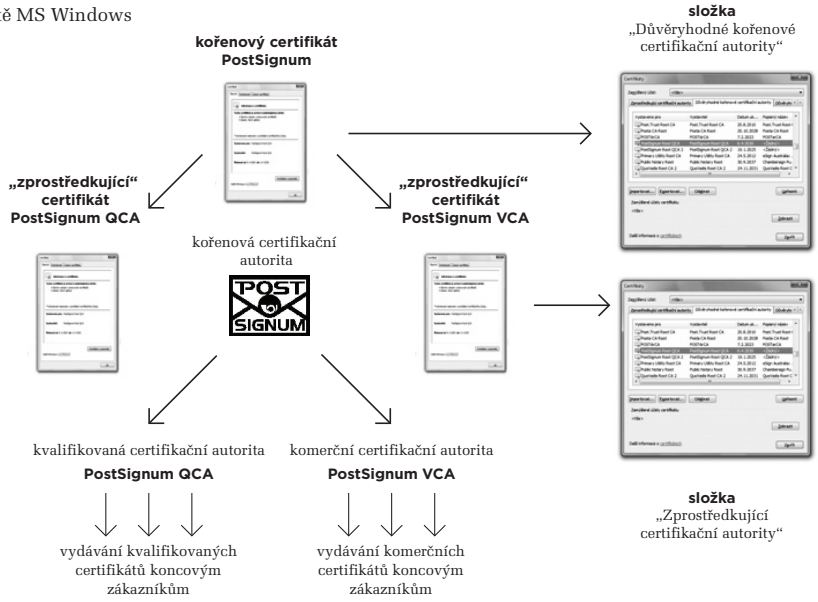
Velmi významná je u systémového úložiště složka „Důvěryhodné kořenové certifikační autority“, kterou je třeba odlišit od složky „Zprostředkující certifikační autority“. Jde o dvojici složek, která umožňuje zohlednit hierarchii certifikátů, kterou používají některé (ale ne všechny) certifikační autority. Do první z těchto složek patří právě a pouze „kořenové“ certifikáty, neboli takové, které jsou opatřeny vlastním podpisem (jsou „self-signed“). Naproti tomu do druhé složky (“zprostředkující …“) patří takové certifikáty, které mají „nad sebou“ jiné nadřazené certifikáty, kterými jsou podepsány.

Ukažme si to na příkladu CA PostSignum, která používá „dvoupatrovou“ hierarchii svých certifikačních autorit (viz část 1.10.2), a tomu odpovídající „dvoupatrovou“ hierarchii svých certifikátů:

- na nejvyšší úrovni je „Kořenová certifikační autorita“, a její (kořenový) certifikát je třeba umístit do složky „Důvěryhodné kořenové certifikační autority“ systémového úložiště MS Windows. Od roku 2010 má CA PostSignum dvě takovéto kořenové certifikační autority (QCA a QCA2), a každá z nich má svůj vlastní kořenový certifikát (PostSignum Root QCA a PostSignum Root QCA 2). Rozdíl mezi nimi je mj. v použití různých hašovacích funkcí (SHA-1 vs. SHA-2), a délce klíčů.
- na nižší úrovni jsou dvě zprostředkující certifikační autority (v terminologii CA PostSignum označované jako „podřízené“), které teprve vydávají certifikáty koncovým zákazníkům: kvalifikovanou certifikační autoritu (PostSignum Qualified CA), která vydává kvalifikované certifikáty, a veřejnou certifikační autoritu (PostSignum Public CA), která vydává komerční certifikáty. Certifikáty těchto zprostředkujících (podřízených) certifikačních autorit se v systémovém úložišti MS Windows umisťují do složky „Zprostředkující certifikační autority“.

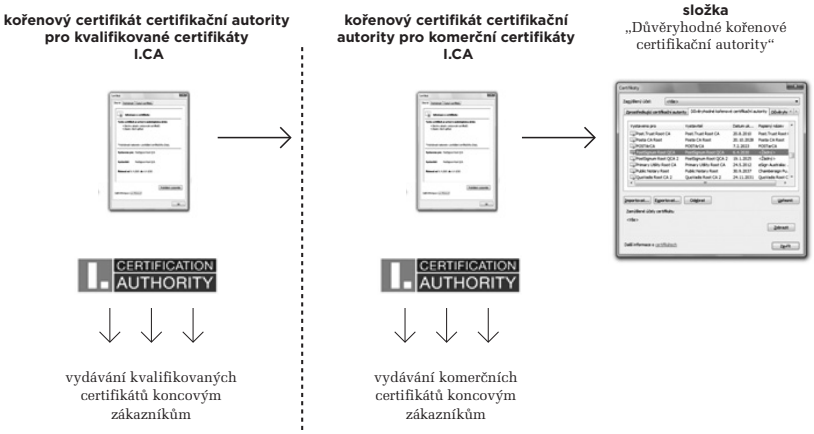
Obrázek 5-30

Správné zařazení certifikátů CA PostSignum do složek systémového úložiště MS Windows



Obrázek 5-31

Zařazení certifikátů I. CA do složek systémového úložiště MS Windows



Poněkud odlišně je tomu v případě I.CA, která nepoužívá hierarchické, ale „ploché“ uspořádání svých jednotlivých certifikačních autorit. Každá z nich tak má svůj vlastní kořenový certifikát (s vlastním podpisem, self-signed), a v systémovém úložišti MS Windows je třeba tyto certifikáty umístit do složky „Důvěryhodné kořenové certifikační autority“.

Jak záhy uvidíme, obě popisované složky („Důvěryhodné kořenové certifikační autority“ a „Zprostředkující certifikační autority“) se určitým způsobem účastní i na automatickém načítání certifikátů. To je společně odlišuje od poslední dosud nepopisované složky „Důvěryhodní vydavatelé“. Do ní by měly být umisťovány certifikáty těch vydavatelů (certifikačních autorit), kterým chceme důvěřovat, ale současně se neúčastní (resp. nemají účastnit) automatického načítání certifikátů.

Pro instalování certifikátů do systémového úložiště MS Windows má uživatel k dispozici průvodce, který nabízí, že za něj vybere správnou složku a do ní certifikát umístí.

> V případě kořenových certifikátů tuzemských akreditovaných certifikačních autorit se ale tento průvodce (hlavně na vyšších verzích MS Windows, jako je Vista a 7) někdy plete a kořenové certifikáty místo do správné složky („Důvěryhodné kořenové certifikační autority“) umisťuje nesprávně do složky („Zprostředkující certifikační autority“).

5.4.3 Počáteční obsah úložišť certifikátů

Snad každé interní úložiště, které si pro své potřeby zřizuje konkrétní program (či operační systém jako takový, v případě systémového úložiště), je již od počátku („od výrobce“) naplněno určitými certifikáty, a dokonce může být i průběžně a zcela automaticky „doplňováno“. Pochopitelně přitom jde výhradně o certifikáty certifikačních autorit, a nikoli o osobní certifikáty konkrétních uživatelů.

Pro uživatele je tato skutečnost velmi podstatná: tvůrce programu tak vlastně „za něj“ vyjadřuje důvěru konkrétním certifikačním autoritám, a to podle svého vlastního uvážení a svých vlastních kritérií. To má významný pozitivní efekt: například když uživatel poprvé „přistoupí“ na nějaký server, který se mu prokáže certifikátem vystaveným některou z takovýchto certifikačních autorit, program sám pozná, že může certifikátu důvěřovat a uživatele „pustí dál“, aniž by se (uživatel) musel o cokoli kolem certifikátů starat.

Současně je zde ale i určité potenciální nebezpečí: uživatel, který pracuje s konkrétním programem, nemusí mít stejná kritéria pro důvěryhodnost certifikačních autorit, jako tvůrce tohoto programu. Sám tedy nemusí považovat za dostatečně důvěryhodnou nějakou certifikační autoritu, kterou tvůrce programu naopak za důvěryhodnou považoval. Pravděpodobnost takovéhoto „rozdílu v názorech“ asi nebude moc velká, ale nelze ji zanedbávat.

Zapomínat bychom neměli ani na právní stránku věci: odpovědnost za případné následky z nesprávného posouzení platnosti konkrétního elektronického podpisu či značky půjde vždy k tíži uživatele, nikoli tvůrce programu.

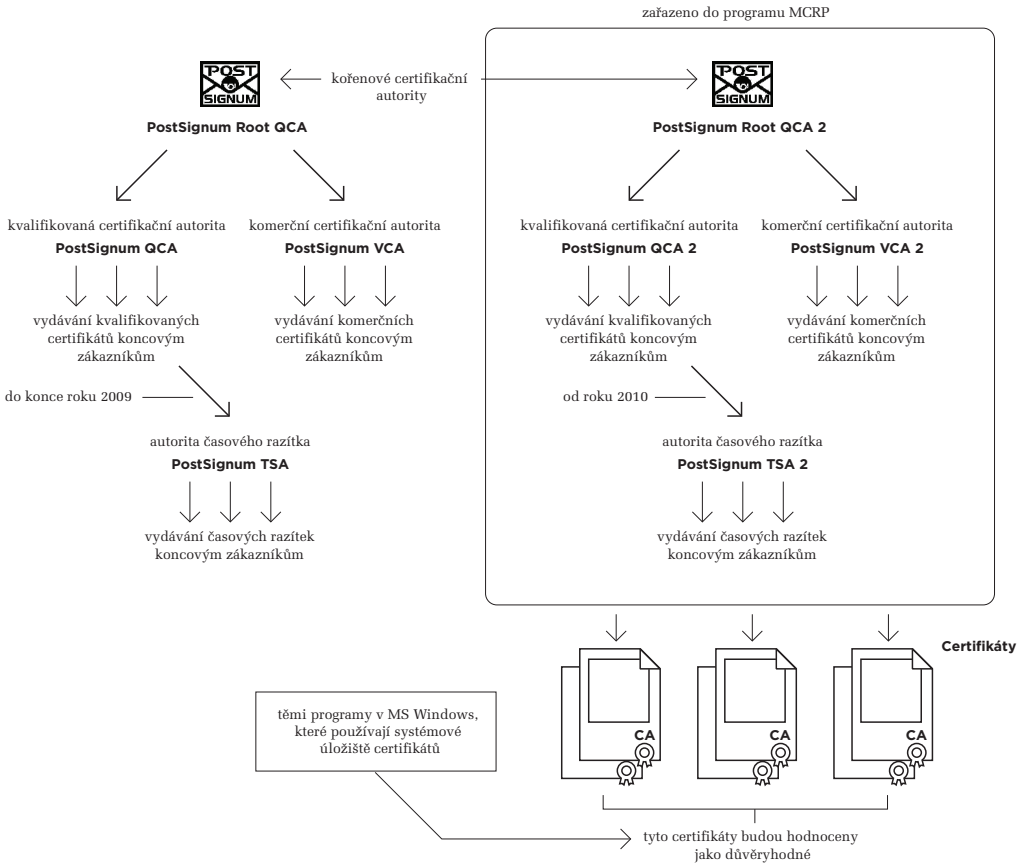
5.4.3.1 Program MRCP společnosti Microsoft

Někteří tvůrci programů vůbec nezveřejňují kritéria, podle kterých vyjadřují svou důvěru konkrétním certifikačním autoritám a jejich certifikáty „předinstalovávají“ do úložišť svých programů. Jinde jsou takováto kritéria známa.

Příkladem může být řešení společnosti Microsoft, které se týká obsahu systémového úložiště v operačních systémech MS Windows. Zde jsou pravidla a podmínky přidávání certifikátů do úložiště předem známy: jde o celý program pro certifikační autority, který společnost Microsoft pojmenovala **MRCP (Microsoft Root Certificate Program)**. Podle svého názvu se týká pouze kořenových certifikátů, ale určitým způsobem zahrnuje i certifikáty podřízených certifikačních autorit, které nejsou kořenové. V zásadě lze konstatovat, že pokud certifikační autorita splní podmínky programu MRCP, jsou její kořenové (a zprostředkovaně i další) certifikáty automaticky zařazovány do systémového úložiště

Obrázek 5-32

Představa dopadu zařazení jednoho z kořenových certifikátů CA PostSignum do programu MRCP



operačního systému MS Windows. Ty programy, které toto systémové úložiště používají, pak automaticky považují za důvěryhodné všechny certifikáty, vydané těmito certifikačními autoritami.

- První tuzemskou certifikační autoritou, která splnila podmínky programu MRCP a byla do něj zařazena (na přelomu května a června 2008) je I.CA. Do programu jsou zařazeny všechny její kořenové certifikáty.
- Druhou tuzemskou certifikační autoritou, která byla zařazena do programu MRCP (ke 24. 5. 2010), je CA PostSignum. Zařazen byl ale pouze její „dvojkový" kořenový certifikát (PostSignum Root QCA 2), vytvořený kvůli přechodu na hašovací funkci SHA-2, a nikoli její původní kořenový certifikát (PostSignum Root QCA).

Konkrétní efekt si můžeme ukázat na předchozím obrázku: ty programy, které běží na platformě MS Windows a které používají systémové úložiště certifikátů tohoto operačního systému (tedy například aplikace z MS Office, prohlížeče Internet Explorer či Google Chrome) budou automaticky považovat za důvěryhodné všechny certifikáty, vydané některou ze „dvojkových" podřízených certifikačních autorit PostSignum, zastřešených novou („dvojkovou") kořenovou certifikační autoritou (PostSignum Root QCA 2). Tedy jak kvalifikované certifikáty, vydané kvalifikovanou certifikační autoritou PostSignum QCA 2, tak i komerční certifikáty vydané komerční autoritou PostSignum VCA 2, i časová razítka vydaná autoritou časového razítka PostSignum TSA (od roku 2010).

> Obecně jsou to všechny certifikáty, jejichž certifikační cesta vede ke kořenovému certifikátu autority PostSignum Root QCA 2.

5.4.3.2 Statut autorit, jejichž certifikáty nejsou zařazeny do úložišť

Na předchozím obrázku si můžeme zdůraznit jednu velmi významnou skutečnost, kterou jsme si nepřímo již několikrát naznačovali: pokud kořenový certifikát nějaké certifikační autority není již „od počátku" zařazen v úložišti certifikátů, rozhodně to neznamená, že by příslušná certifikační autorita byla nedůvěryhodná, a tím byly nedůvěryhodné i všechny certifikáty, vydané touto autoritou či některou z jí podřízených autorit.[10]

> V případě CA PostSignum to tedy neznamená, že by certifikáty vydané původními podřízenými certifikačními autoritami CA PostSignum (PostSignum QCA, PostSignum VCA, na obrázku vlevo) byly nedůvěryhodné.

To, že (některé či všechny) certifikáty nějaké konkrétní certifikační autority nejsou zařazeny do „počáteční náplně" používaného úložiště certifikátů, můžeme interpretovat pouze tak, že o jejich důvěryhodnosti

---

[10] Za nedůvěryhodné můžeme považovat pouze ty certifikáty, které jsou uloženy ve složce „Nedůvěryhodní vydavatelé" v systémovém úložišti MS Windows, viz výše, nebo od nich odvozené certifikáty (tj. certifikáty jejichž certifikační cesta vede k těmto nedůvěryhodným certifikátům).

nejsou k dispozici žádné informace. Tím pádem nejsou k dispozici žádné informace ani o věrohodnosti certifikátů, které takováto certifikační autorita vydala.[11]

> Pro dokreslení si uvědomme, že žádný tvůrce programu, který připravuje „počáteční výbavu“ úložiště certifikátů pro svůj program, nemá z principu šanci posoudit důvěryhodnost všech již existující certifikačních autorit a rozhodnout o zařazení jejich kořenových certifikátů do svého úložiště. Natož pak důvěryhodnost kořenových certifikátů, které teprve budou vydány. Proto může do „počáteční výbavy“ zařadit jen některé kořenové certifikáty a nikoli všechny.

Zdůrazněme si ještě jednou, že nedostatek informací k posouzení se nerovná tomu, že něco je nedůvěryhodné.

Pravdou ale je, že nejrozšířenější webové prohlížeče tuto důležitou skutečnost až tolik nerespektují. Pokud totiž narazí na server, který se jim prokazuje takovým certifikátem, u kterého nedokáží posoudit jeho důvěryhodnost, chovají se skoro tak, jako kdyby šlo rovnou o nedůvěryhodný server.

Prohlížeče uživatele před vstupem na takovýto server varují (což je na místě), ale zdůvodnění tohoto varování není správné. Místo upozornění na nedostatek informací vytváří dojem, že jde o nedůvěryhodný či přímo podvodný server. To může být, ale také nemusí být pravda. A nedává to uživateli dostatečně najevo, že je na něm, aby dodal chybějící informace.

> Asi nejlépe to bylo patrné při spuštění datových schránek v roce 2009. Server, na kterém běžel webový portál informačního systému datových schránek (ISDS), se prohlížeči prokazoval pomocí (systémového) certifikátu, který mu vystavila ještě původní („jedničková“) CA PostSignum (tj. PostSignum Root QCA). Příslušný kořenový certifikát této certifikační autority ale nebyl součástí „počáteční výbavy“ důvěryhodných certifikátů žádného prohlížeče (ani systémového úložiště MS Windows). A tak – pokud si jej uživatel nedoplnil sám – jeho prohlížeč ho před vstupem na webový portál ISDS varoval, jako kdyby šlo o nedůvěryhodný server. Jak, to ukazují dva obrázky na následující stránce.

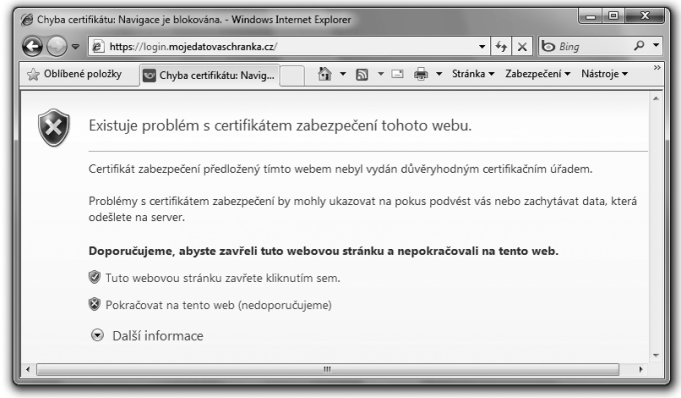
Jako uživatelé bychom tedy měli chápat „počáteční výbavu“ každého úložiště certifikátů jen jako určitý základ, na kterém bychom měli dále pracovat. Tedy doplňovat ho o další certifikáty, kterým my sami chceme důvěřovat.

Žádná „počáteční výbava“ ale nemůže být nikdy úplná. Přesto má svůj význam, protože dokáže uživatelům – zvláště těm méně zkušeným – usnadnit život tím, že nemusí sami přidávat různé „dobře známé“ certifikační autority (přesněji ty, které jako důvěryhodné vybral již tvůrce programu).

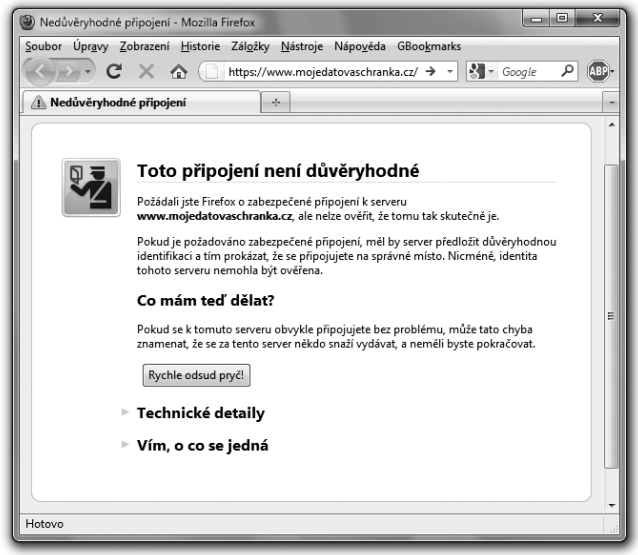
---

[11] Zcela přesně bychom měli hovořit o certifikátech, jejichž elektronická značka je založena na předmětném certifikátu certifikační autority. Jedna a táž certifikační autorita totiž může vydávat různé certifikáty a podepisovat (označovat) je s využitím různých svých certifikátů.

Obrázek 5-33
Reakce Internet Exploreru na serverový certifikát, jehož důvěryhodnost nedokáže posoudit



Obrázek 5-34
Reakce Firefoxu na serverový certifikát, jehož důvěryhodnost nedokáže posoudit



> Pokud by se Česká pošta bývala včas dohodla s Microsoftem na zařazení kořenového certifikátu její CA PostSignum do programu MRCP (a tím i do „počáteční výbavy“) systémového úložiště v MS Windows, nemusela by alespoň část uživatelů datových schránek při prvním přístupu narážet na varování prohlížeče (viz výše).[12]

[12] Konkrétně ti uživatelé, kteří používají operační systém Windows a prohlížeč Internet Explorer.

Existence „počáteční výbavy“ úložišť certifikátů má ale i své nástrahy. Kritéria důvěryhodnosti, které aplikuje autor programu, se nemusí nutně shodovat s kritérii, která hodlá aplikovat uživatel. Ten to pak může řešit i tak, že některé certifikáty z „počáteční výbavy“ zase smaže.

> Extrémem je pak takový přístup, kdy uživatel vůbec nedůvěřuje tomu, co za něj vybral a prohlásil za důvěryhodné autor programu. Všechny certifikáty z „počáteční výbavy“ proto nejprve odstraní, a teprve pak začne plnit úložiště takovými certifikáty, které si vybral (a považuje za důvěryhodné) on sám.

5.4.3.3 Program AATL společnosti Adobe

Program MRCP společnosti Microsoft je zřejmě nejrozsáhlejším, ale nikoli jediným svého druhu. Obdobné programy postupně zavádí i další producenti systémového i aplikačního softwaru.

Například společnost Adobe si vytvořila obdobně koncipovaný program **AATL (Adobe Approved Trust List)**, který využívají její produkty. Konkrétně jde o Adobe Reader a Adobe Acrobat, které podporují program AATL od své verze 9.

Svým „rozsahem“ je program AATL výrazně skromnější než program MRCP, a odlišný je i konkrétní mechanismus jeho fungování (podrobněji viz část 5.4.4.1). V roce 2010 bylo v programu AATL jen 10 certifikačních autorit, mezi kterými ale nebyla žádná z ČR.

5.4.4 Přidávání dalších certifikátů do úložišť důvěryhodných certifikátů

Přidat (vložit, nainstalovat) nový certifikát do konkrétního úložiště certifikátů, a tím mu vyjádřit svou důvěru, je v principu velmi jednoduché. Tedy alespoň: je to jednoduché v situaci, kdy již máme „v ruce“ příslušný certifikát a máme jistotu, že jde skutečně o „ten správný“ certifikát. Pak již stačí jen využít některou z možností pro vkládání (resp. import) certifikátů, které jsou pro dané úložiště k dispozici.

> Určitou nástrahou přesto je volba správné složky (v rámci daného úložiště) pro instalaci nového certifikátu, viz část Určitou nástrahou přesto je volba správné složky (v rámci daného úložiště) pro instalaci nového certifikátu, viz část 5.4.2: pozor musíme dávat zejména na kořenové certifikáty certifikačních autorit, jejich podřízené certifikační autority, ale i na osobní certifikáty.

To, co je na přidávání certifikátů vlastními silami těžké, jsou spíše jiné věci. Nejprve výběr těch certifikátů, které by měly být přidány, a pak dostatečně důvěryhodný způsob jejich získání.

S tím pak souvisí ještě jeden nesmírně důležitý aspekt: způsob fungování konkrétního úložiště certifikátů. To si totiž může (dodatečně, nad rámec své „počáteční výbavy“) instalovat některé certifikáty samo, z vlastní iniciativy, a dokonce bez toho, že by to uživateli dalo najevo a chtělo k tomu od něj souhlas. Někdy to dokonce dělá i navzdory tomu, co si uživatel přeje.

Začněme proto právě u automatického přidávání (instalování) certifikátů do různých úložišť certifikátů.

K tomu může docházet ze dvou principiálních důvodů, které se týkají různých certifikátů:

- v souvislosti s „počáteční výbavou“ příslušného úložiště: tato možnost se týká kořenových certifikátů důvěryhodných certifikačních autorit
- přidáváním těch certifikátů, které leží na důvěryhodné certifikační cestě: tato možnost se týká zprostředkujících (tj. nikoli kořenových) certifikátů certifikačních autorit.

5.4.4.1 Automatické přidávání kořenových certifikátů

Jak již víme, každý producent programu, který používá vlastní úložiště certifikátů, pro něj připravuje nějakou „počáteční výbavu“ kořenových certifikátů důvěryhodných certifikačních autorit. Tu ale nemusí instalovat vždy celou a najednou, při instalaci samotného programu. Již jen proto, že musí být pamatováno i na změny (na vznik nových důvěryhodných certifikačních autorit, na eventuálníztrátu důvěryhodnosti, ale třeba také na pravidelnou obměnu certifikátů certifikačních autorit). Proto nemůže být řešení s „počáteční výbavou“ úplně statické.

Ukázat si to můžeme na příkladu systémového úložiště v MS Windows. Zde je ale situace značně odlišná podle toho, zda jde o Windows XP, nebo novější verzi (Vista či Windows 7):

> Když si na svém počítači nově nainstalujete Windows XP, ihned najdete v systémovém úložišti tohoto operačního systému velký počet kořenových certifikátů certifikačních autorit, téměř 230. Další se pak mohou přidávat v rámci v rámci mechanismů aktualizace MS Windows (různých aktualizačních balíčků a „záplat“). V zásadě – až na tyto aktualizace – ale jakoby platil obecný princip: „vše je již na vašem počítači“.
>
> V případě MS Vista a vyšších verzí MS Windows je situace jiná: při instalaci samotného operačního systému se do systémového úložiště uloží jen několik málo důvěryhodných kořenových certifikátů certifikačních autorit. Ostatní certifikáty, které tvůrce operačního systému (společnost Microsoft) považuje za důvěryhodné a zařazuje do svého programu MRCP (Microsoft Root Certificate Program), zůstávají dostupné on-line, na serverech Microsoftu.
>
> Když se pak má posoudit důvěryhodnost nějakého konkrétního certifikátu, nejprve se najde příslušná certifikační cesta, neboli posloupnost certifikátů, vedoucí od posuzovaného certifikátu až k některému kořenovému certifikátu. Tento kořenový certifikát se pak nejprve hledá v systémovém úložišti na daném počítači. Pokud se v něm nenajde, hledá se dále on-line, na serverech Microsoftu, mezi důvěryhodnými certifikáty v rámci programu MRCP. Pokud je kořenový certifikát nalezen zde, je doinstalován (jako důvěryhodný kořenový certifikát) do příslušného systémového úložiště na daném počítači. A to automaticky, aniž by byl uživatel dotazován na souhlas či o tom byl jen informován.[13]

---

[13] Smyslem tohoto řešení, shodného pro Windows XP i vyšší verze, je zřejmě zefektivnění správy certifikátů (které se instalují až v okamžiku skutečné potřeby) a maximální odlehčení uživatele, který se nemusí o nic starat.

Tímto chováním lze mj. vysvětlit i disproporci mezi tím, že uživatel nejprve vůbec nenajde nějaký konkrétní kořenový certifikát v systémovém úložišti svého operačního systému, ale programy, které toto úložiště používají, budou „samy od sebe“ důvěřovat všem certifikátům příslušné certifikační autority: při prvním přístupu je její kořenový certifikát automaticky doinstalován.

Mechanismy pro takovéto automatické instalování důvěryhodných kořenových certifikátů dokonce „přebíjejí“ vůli uživatele: pokud ten sám smaže některý z kořenových certifikátů ze systémového úložiště MS Windows, je tento certifikát při nejbližší relevantní příležitosti zase znovu automaticky nainstalován.[14]

> Připomeňme si ještě, že z tuzemských (akreditovaných) certifikačních autorit je do programu MRCP společnosti Microsoft zařazena certifikační autorita I.CA (se všemi kořenovými certifikáty, které používá), a částečně i CA PostSignum (ale jen svým novým kořenovým certifikátem, neboli certifikátem PostSignum Root QCA 2 své nové „dvojkové“ kořenové autority).
>
> Stejně tak si připomeňme, že popisované automatické dočítání kořenových certifikátů se týká pouze systémového úložiště operačního systému MS Windows a ovlivňuje tak chování pouze těch programů, které toto úložiště využívají.

Poněkud odlišně to funguje u Adobe Readeru (i Acrobatu) od společnosti Adobe, která má svůj vlastní program AATL (Adobe Approved Trust List), týkající se pouze kořenových certifikátů, viz část 5.4.3.3:

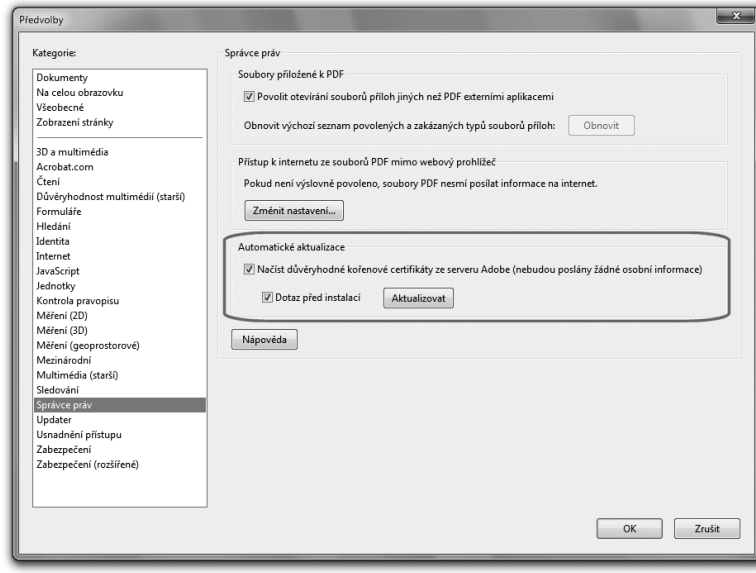
> Kořenové certifikáty, zařazené do programu AATL, tvoří jednorázovou „počáteční náplň“ vlastního úložiště Readeru při instalaci tohoto programu. Uplatňují se ale i při průběžné aktualizaci obsahu tohoto úložiště: Reader si každých 90 dnů stahuje aktuální verzi tohoto seznamu, a z něj si pak doplňuje ty kořenové certifikáty, které mu v úložišti chybí.[15]
>
> Na rozdíl od mechanismů aktualizace kořenových certifikátů v operačním systému MS Windows má u Adobe Readeru uživatel větší kontrolu nad celým procesem aktualizace. Může ho zakázat, prostřednictvím standardního uživatelského nastavení (viz následující obrázek). Nebo ho může naopak explicitně vyvolat, aby nemusel čekat na příští plánovanou aktualizaci po 90 dnech.

---

[14] Existuje možnost vypnutí popisovaného automatického doinstalovávání kořenových certifikátů: na MS Windows XP odinstalováním systémové komponenty „Aktualizace kořenových certifikátů“, a na MS Windows Vista a vyšších skrze podporu zásad skupiny, případně přímo editací registru: vytvořením DWORD položky DisableRootAutoUpdate ve složce HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot a jejím nastavením na hodnotu 1.

[15] Přesněji aktuální verzi seznamu stahuje až v okamžiku, kdy má ověřit podpis na nějakém podepsaném dokumentu.

Obrázek 5-35
Uživatelské nastavení aktualizace kořenových certifikátů u Adobe Readeru



5.4.4.2 Automatické přidávání podřízených certifikátů

Druhá možnost automatického přidávání certifikátů do konkrétního úložiště se již týká „podřízených“ certifikátů, které patří podřízeným (zprostředkujícím) certifikačním autoritám. Tedy takových certifikátů, které leží na certifikační cestě ke kořenovému certifikátu. V praxi jde o certifikáty, které se v systémovém úložišti MS Windows instalují odděleně od kořenových certifikátů, do složky pro „zprostředkující certifikační autority“.

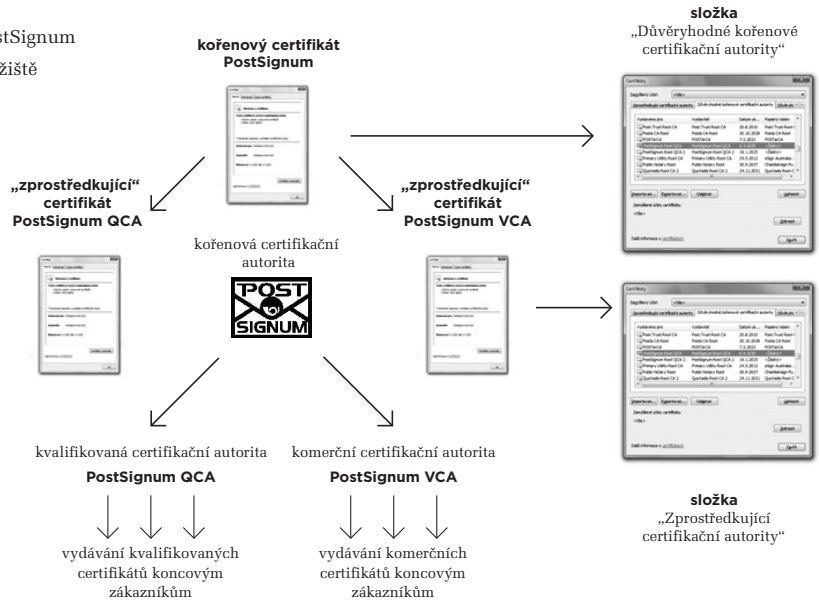
> V roli příkladu si zopakujme strukturu certifikačních autorit, se kterou pracuje CA PostSignum, a kterou jsme si naposledy ukazovali v části 5.4.2.3 jako obrázek 5-30, nyní viz obrázek 5-36 na následující stránce.
>
> Zde se tedy jedná o certifikáty podřízených autorit: kvalifikované PostSignum QCA a veřejné PostSignum VCA. Nebo jejich „dvojkových“ verzí (PostSignum QCA 2 a PostSignum VCA 2).

Smyslem automatického přidávání těchto podřízených certifikátů (certifikátů podřízených, resp. zprostředkujících autorit) je usnadnit a zjednodušit plnění příslušného úložiště: aby do něj nemusely být dopředu (či nějak „ručně“) přidávány všechny podřízené certifikáty, které by kdy mohly být zapotřebí. Stejně tak je tímto způsobem pamatováno na to, že struktura podřízených certifikačních autorit se může měnit přeci jen častěji, stejně jako jejich certifikáty, zatímco struktura kořenových certifikačních autorit se až tak často nemění (stejně jako kořenové certifikáty těchto autorit).

Abychom toto tvrzení docenili, uvědomme si zásadní rozdíl mezi přidáním nového kořenového certifikátu a nového podřízeného (zprostředkujícího) certifikátu:

- v případě přidání kořenového certifikátu se mění (zvětšuje) „rozsah“ vyjádřené důvěry
- v případě přidání podřízeného certifikátu (certifikátu podřízené autority) se „rozsah“ vyjádřené důvěry nemění.

Obrázek 5-36
Zařazení certifikátů CA PostSignum do složek systémového úložiště MS Windows

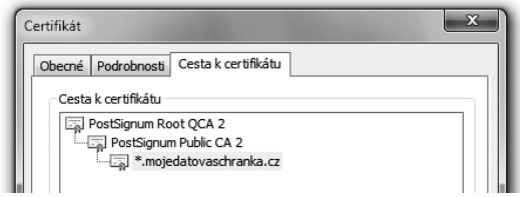


K automatickému přidání nového podřízeného certifikátu totiž dochází pouze v případě, kdy již je nainstalován (a tím i považován za důvěryhodný) odpovídající kořenový certifikát. Opět si to ukažme na konkrétním příkladu.

> Nechť je v úložišti důvěryhodných certifikátů již nainstalován nový „dvojkový“ kořenový certifikát CA PostSignum (PostSignum Root QCA 2). Lhostejno zda skrze automatické přidávání kořenových certifikátů do systémového úložiště v MS Windows, či díky „ručnímu“ přidání uživatelem.

Když pak uživatel přistoupí na nějaký server – například na webový portál ISDS – ten se mu prokáže serverovým (komerčním) certifikátem, vydaným novou komerční (podřízenou) certifikační autoritou PostSignum (PostSignum Public CA 2). Při zkoumání důvěryhodnosti tohoto certifikátu je nejprve vyhledána certifikační cesta, vedoucí k některému kořenovému certifikátu. Ta je nalezena v následující podobě:

- kořenový certifikát (kořenové autority PostSignum Root QCA 2)
- podřízený certifikát (podřízené autority PostSignum Public CA 2)
- posuzovaný certifikát (pro server na adrese *.mojedatovaschranka.cz)



Obrázek 5-37
Příklad certifikační cesty, z pohledu posuzovaného cerfifikátu

> Jelikož tato certifikační cesta „končí“ takovým kořenovým certifikátem, který je považován za důvěryhodný (nachází se v příslušné části úložiště důvěryhodných certifikátů), může hodnotící program (prohlížeč) považovat posuzovaný serverový certifikát za důvěryhodný a uživatele pustit na stránky tohoto serveru.
>
> Současně s tím může být považován za důvěryhodný i podřízený certifikát (zde PostSignum Public CA2), který dosud není umístěn v příslušné části úložiště důvěryhodných certifikátů – a tak sem může být dodatečně (a automaticky) přidán.

Připomeňme si znovu, že toto automatické přidávání podřízených certifikátů nemění „rozsah důvěry“, a je tedy spíše optimalizačním opatřením: urychluje a zefektivňuje následné posuzování důvěryhodnosti dalších konkrétních certifikátů.

Jde přitom o funkčnost, která dnes již není omezena jen na systémové úložiště MS Windows, popisované výše. Své mechanismy pro „dočítání“ certifikátů má například i úložiště, se kterým pracuje prohlížeč Firefox.

5.4.4.3 Ruční přidávání certifikátů

Z předchozích odstavců vyplývá, že konkrétní úložiště důvěryhodných certifikátů mohou měnit svůj obsah bez přímé spoluúčasti uživatele, a vlastně i bez jeho vědomí. Konkrétní způsob, jakým tak činí, přitom nemusí být příliš dobře popsán v dostupných zdrojích. Navíc se vše může ještě dynamicky měnit, s tím jak příslušní producenti softwaru inovují své produkty a v rámci toho mohou měnit i způsob jejich práce s certifikáty a úložišti.

A aby vše bylo ještě komplikovanější, různá úložiště se v tomto ohledu mohou chovat různě: jinak se chová systémové úložiště v MS Windows, jinak to, se kterým pracuje prohlížeč Firefox, a ještě jinak vlastní úložiště Adobe Readeru atd.

V praxi je proto stále velmi důležité, jakým způsobem si uživatel právě používané úložiště certifikátů „zabydlí“ sám. Již jen proto, že jakékoli případné následky (hlavně ty právní) ponese pouze on sám, a nikoli autor programu a pravidel, podle kterých se obsah úložiště mění „sám od sebe“.

Na místě je tedy určitě obezřetnost, doprovázená snahou pochopit, jak se chová to úložiště, se kterým pracuje právě používaný program.

Při „ruční“ instalaci certifikátů do jakéhokoli úložiště je navíc vhodné se příliš nespoléhat na různé automatické funkce. Když už budete přidávat do svého úložiště nějaké kořenové certifikáty (třeba právě ten či ty od CA PostSignum), je vhodné spolu s nimi přidat i všechny jim podřízené (zprostředkující) certifikáty – než se spoléhat na to, že budou přidány automaticky výše popsaným způsobem.

Ovšem to nejdůležitější, a asi i nejtěžší na „ručním“ přidávání jakýchkoli certifikátů do jakéhokoli úložiště je ověření, že skutečně přidáváte ty správné certifikáty. Tedy že se nejedná o nějaké podvrhy, které vám někdo podstrčil, aby vás tím podvedl.

> Jen si zkuste představit důsledky: pokud byste si do svého úložiště důvěryhodných certifikátů uložili nějaký podvržený (kořenový) certifikát, byly by automaticky považovány za důvěryhodné všechny certifikáty, odvozené od tohoto kořenového certifikátu (ve smyslu stromu důvěry). Což by nejspíše byly nějaké phishingové weby a podobné záležitosti, které by se vám následně jevily jako zcela důvěryhodné a bezpečné.

Získání „skutečně pravého“ certifikátu ale není vůbec jednoduché. Jednoznačně nejspolehlivější je získat kořenový certifikát konkrétní certifikační autority přímo od ní, tak že si zajdete do nějaké její provozovny a zde si certifikát necháte nahrát například na svůj USB flash disk. Případně, pokud by se jednalo o nějaký osobní certifikát, když by vám ho dala sama dotyčná osoba, kterou dobře znáte.

Jinak samozřejmě existují i jiné, mnohem „pružnější“ metody, jako třeba stažení kořenového certifikátu přímo z Internetu, z webových stránek příslušné certifikační autority. Takto je nabízí každá z nich. Zde si ale musíme uvědomit riziko, které je s tím spojeno: jste si opravdu jisti, že si kořenový certifikát stahujete skutečně ze stránek příslušné certifikační autority a nikoli z nějakého podvodného webu, který se za takovéto stránky pouze vydává? A to třeba právě proto, aby vám podstrčil svůj podvodný certifikát místo toho správného?

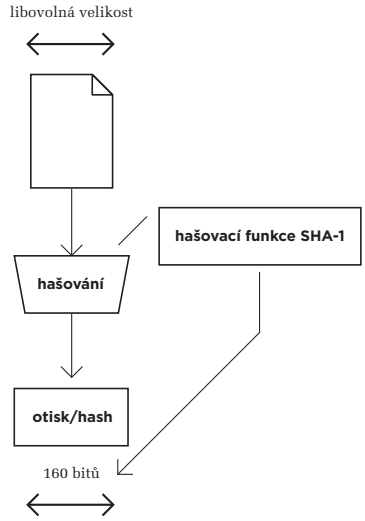
Pokud vám takováto možnost přijde absurdní, pak si ji srovnejte s nebezpečím phishingu. Ten také předpokládá, že se uživateli podstrčí stránky, které vypadají úplně stejně jako stránky jeho banky, aby na nich zadal přístupové údaje ke svému účtu. A statistiky bohužel dokládají, že to funguje.

Naštěstí v případě kořenových certifikátů, které si stáhnete z webu, máte ještě možnost dodatečného ověření, zda jste si stáhli správné certifikáty. A to přes jejich otisky (hash-e), které si můžete zkontrolovat i podle jiných zdrojů.

> Připomeňme si to, co jsme si již popisovali v části 2.5: jak se z libovolně velkého dokumentu nejprve vytváří otisk (hash), který již má pevnou velikost, a teprve ten se pak podepisuje.
>
> Otisky ale nemusíme vytvářet jen z elektronických dokumentů. Stejně tak lze vytvořit otisk i z certifikátu, který je vlastně také takovým elektronickým dokumentem, resp. zprávou. Jeho otisk pak může sloužit pro kontrolu toho, zda jde skutečně o ten správný certifikát.

Připomeňme si také, že jednou z podstatných vlastností každé hašovací funkce je to, že při libovolné změně původního dokumentu vychází otisk jiný. Díky tomu je možné zajistit integritu dokumentu, resp. rozpoznat každou jeho změnu. Tedy i změnu obsahu certifikátu.

Obrázek 5-38
Představa hašování (s hašovací funkcí SHA-1)



Příklad (skutečného) otisku kořenového certifikátu (konkrétně certifikátu PostSignum Root QCA 2), vytvořeného pomocí hašovací funkce SHA-1, je:

SHA-1: A0F8 DB3F 0BF4 1769 3B28 2EB7 4A6A D86D F9D4 48A3

Kde ale získat správné hodnoty otisků, a jak je správně porovnat s otisky těch certifikátů, které jsme si odněkud stáhli?

Na první otázku by se dalo odpovědět tak, že tyto hodnoty se dají získat přímo z webu příslušných certifikačních autorit. Ale to je stejně (ne)spolehlivý zdroj jako pro stahování samotných certifikátů. To už je pak přeci jen o něco bezpečnější najít si hodnoty otisků na jiném webu, než ze kterého byly staženy certifikáty. Protože šance na souběžné podvržení dvou webů je přeci jen o něco menší, než šance na podvržení jen jednoho.

Otisky našich akreditovaných certifikačních autorit můžete najít také na webu MV ČR, který je dozorovým orgánem v oblasti elektronického podpisu,[16] a který ověřuje i jejich certifikáty.

[16] Na zcela nevhodné (příliš dlouhé) URL adrese: *http://www.mvcr.cz/clanek/vysledky-overeni-platnych-kvalifikovanychsystemovych-certifikatu-akreditovanych-poskytovatelu-certifikacnich-sluzeb.aspx*

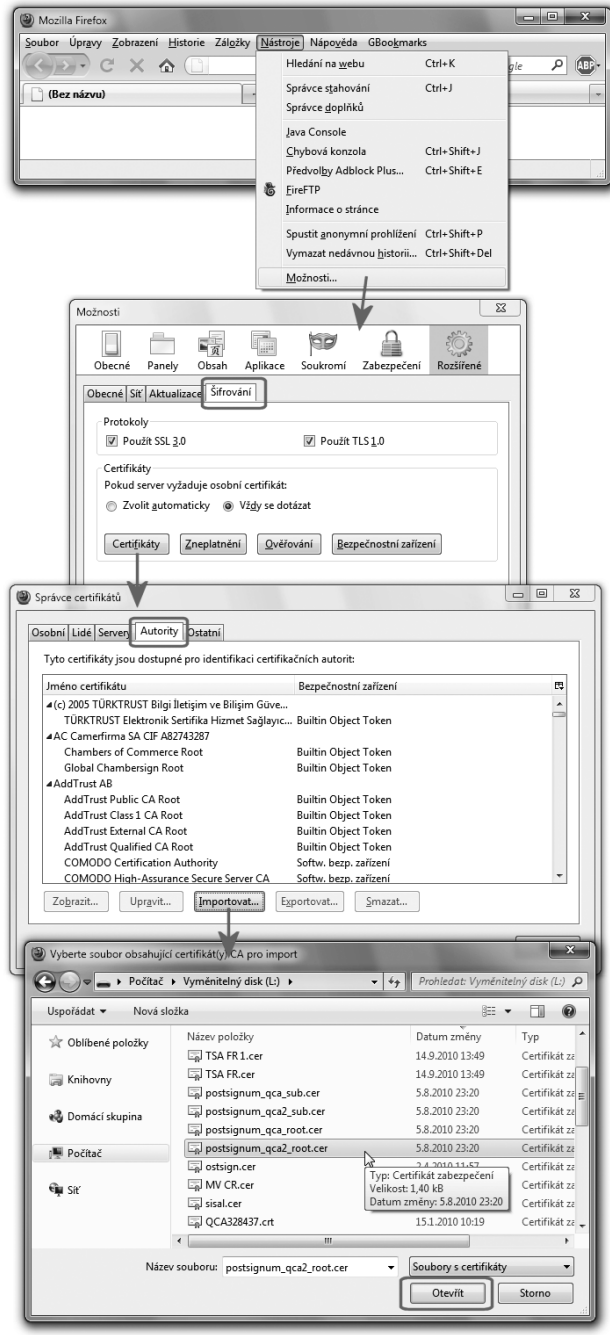
Obrázek 5-39
Příklad výsledku ověření kořenového certifikátu PostSignum Root QCA 2

Poř. číslo	Ověření kvalifikovaného systémového certifikátu poskytovatele			
	Subjekt		Adresa	
20.	**Česká pošta, s. p.** **identifikační číslo 47 11 49 83**		Olšanská 38/9, PSČ 225 99 Praha 3	
Výsledky ověření ze dne 27. 1. 2010				
A.	Jméno	postsignum_qca2_root.pem	**sér. č.: 100**	Délka: 2004 byte
	Formát certifikátu		**Otisk**	
	PEM	MD5	E3CD A846 DEEA 8FD3 781F B720 C4FC DB5C	
		SHA-1	B680 B039 517B B935 D691 25EF 958C 75DD 1A42 4D37	
		SHA-256	9527 2929 1C6D 55EF 53E7 B6EE 2207 04F1 F400 561E D8B7 A6DE 047A 29C1 1E27 E0C2	
B.	Jméno	postsignum_qca2_root.der	**sér. č.: 100**	Délka: 1440 byte
	Formát certifikátu		**Otisk**	
	DER	MD5	5973 6628 512B 98B4 10FF 7D06 FA22 D6C8	
		SHA-1	A0F8 DB3F 0BF4 1769 3B28 2EB7 4A6A D86D F9D4 48A3	
		SHA-256	AD01 6F95 8050 E0E7 E46F AE7D CC50 197E D8E3 FF0A 4B26 2E5D DCDB 3EDD DC7D 6578	
C.	Jméno	postsignum_qca2_root.txt	**sér. č.: 100**	Délka: 3948 byte
	Formát certifikátu		**Otisk**	
	TXT	MD5	ED3F A8B7 C7A4 7CA1 797A 3767 AC26 0A1C	
		SHA-1	4621 E9C1 E862 7716 F28E E61E B6C2 3013 7DBB 7454	
		SHA-256	0285 0E43 B3DD 6075 2EB4 5AF9 83F6 C25F 9303 B995 2B9B 69CB 8B98 2E35 F851 FD4E	

Další možností je získat výsledek ověření (i s otisky kořenových certifikátů) ze strany MV ČR v tištěné podobě, formou věstníku MV ČR, kde je pravidelně publikován (a je k dispozici i v PDF na stránkách MV ČR). Ještě další možností je zavolat si do příslušné certifikační autority telefonem a požádat je o ověření správné hodnoty otisku.

> Na jaře 2010, když si informační systém datových schránek (ISDS) pořídil nový serverový certifikát, vycházející z nového („dvojkového“) kořenového certifikátu CA PostSignum (tj. PostSignum Root QCA2), byl tento nový kořenový certifikát rozesílán v datové zprávě do všech datových schránek.

Obrázek 5-40
Příklad postupu při vkládání nového certifikátu do úložiště prohlížeče Firefox



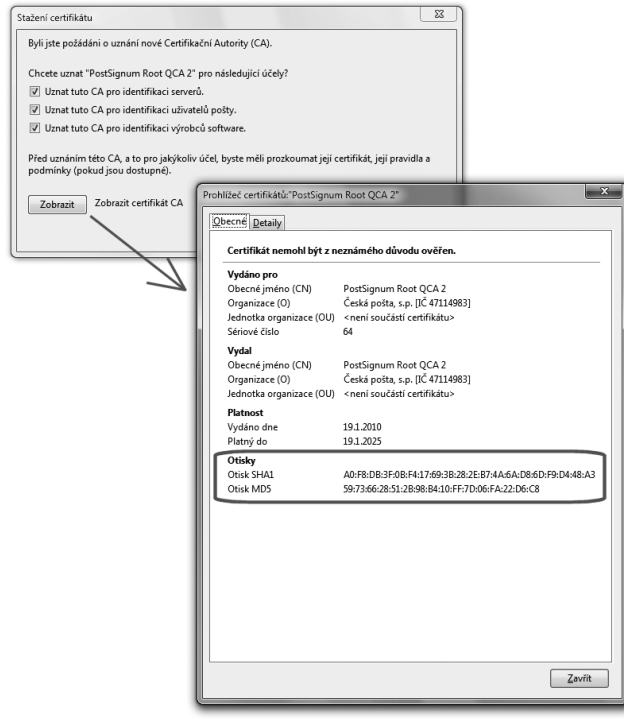
A když už znáte správnou hodnotu otisku, jakým způsobem zjistíte, zda se shoduje s hodnotou otisku toho certifikátu, který se právě chystáte instalovat?

To už je docela snadné: když přidáváte nějaký kořenový certifikát do konkrétního úložiště, snad vždy vám příslušný program, skrze který tak činíte, ukáže jím vypočítaný otisk certifikátu a očekává od vás jeho porovnání se správnou hodnotou. Neučiní tak pouze v případě, kdy stejný certifikát (se stejným otiskem) již je v úložišti nainstalován.

Ukažme si to na konkrétním příkladu přidání nového kořenového certifikátu do úložiště prohlížeče Mozilla Firefox. Celý příklad si ale rozdělíme do dvou etap, znázorněných na dvou samostatných obrázcích. První z nich (na předchozí stránce) ukazuje postup přidávání nového certifikátu a zahrnuje i volbu souboru, ve kterém je certifikát uložen.

Druhý obrázek již ukazuje reakci programu (zde: prohlížeče Firefox), který má vložit nový certifikát jako kořenový do svého úložiště.

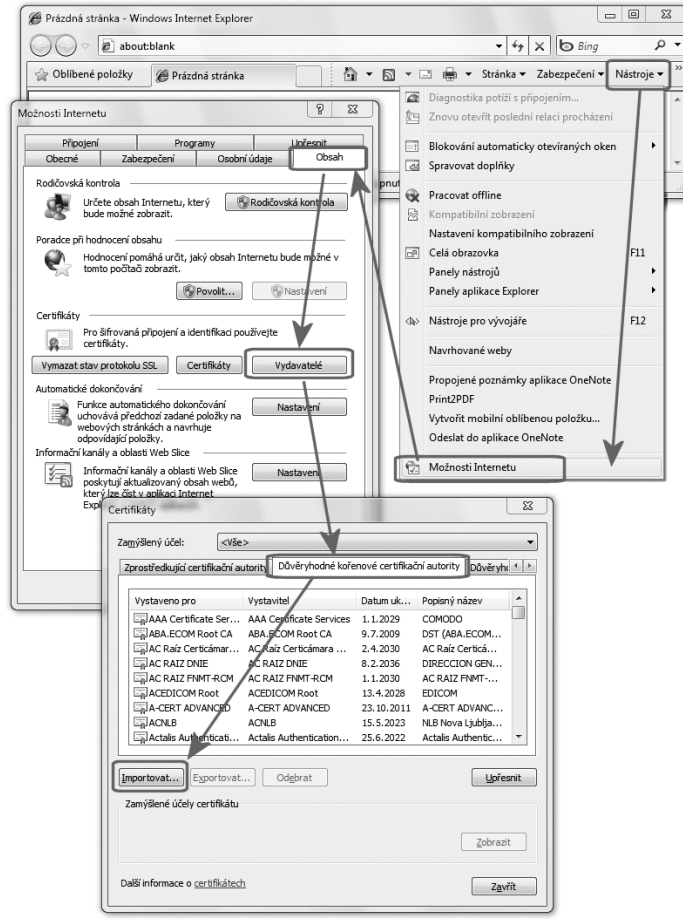
Obrázek 5-41
Příklad kontroly hodnoty otisku právě instalovaného certifikátu



Zde konkrétně jde o nový kořenový certifikát PostSignum Root CA 2. Pro kontrolu si srovnejte správnou hodnotu otisku tohoto certifikátu (získanou pomocí hašovací funkce SHA-1) s hodnotou uvedenou v předchozích příkladech.

Na právě uvedeném příkladu si ještě povšimněte jednoho zajímavého aspektu, který ukazuje horní (levý) obrázek na předchozí straně: při přidávání certifikátu do úložiště je uživatel dotazován na účely jeho využití (podrobněji viz část 4.3.1).

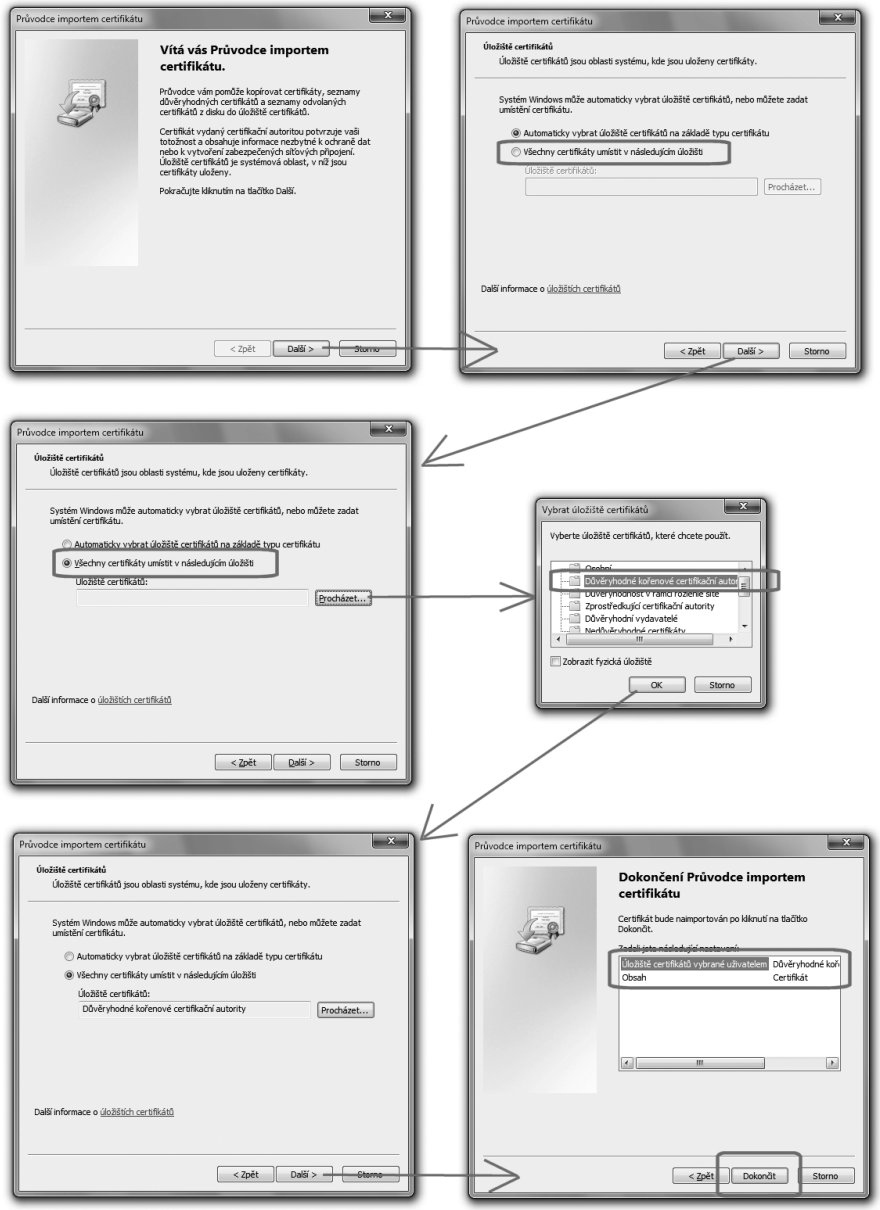
Dalším příkladem, který si zde ukážeme, je přidání nového kořenového certifikátu do systémového úložiště MS Windows, a to prostřednictvím prohlížeče Internet Explorer. Opět to bude na dvě části: první z nich ukazuje začátek postupu, který již – podobně jako u předchozího příkladu – zahrnuje i volbu složky, do které má být nový certifikát instalován.



Obrázek 5-42
Příklad (začátku) přidávání nového certifikátu do systémového úložiště MS Windows, skrze prohlížeč Internet Explorer

Konkrétně jde o složku „Důvěryhodné kořenové certifikační úřady“, kde je následně zvolena možnost importu certifikátu.

Popsaným způsobem se přitom dostaneme v zásadě do stejné situace, jako když si prostředky MS Windows (například skrze Průzkumníka) necháme zobrazit příslušný certifikát, a pak zvolíme možnost „nainstalovat certifikát“. V obou případech je totiž spuštěn průvodce, který uživatele provede instalací certifikátu (do systémového úložiště MS Windows).



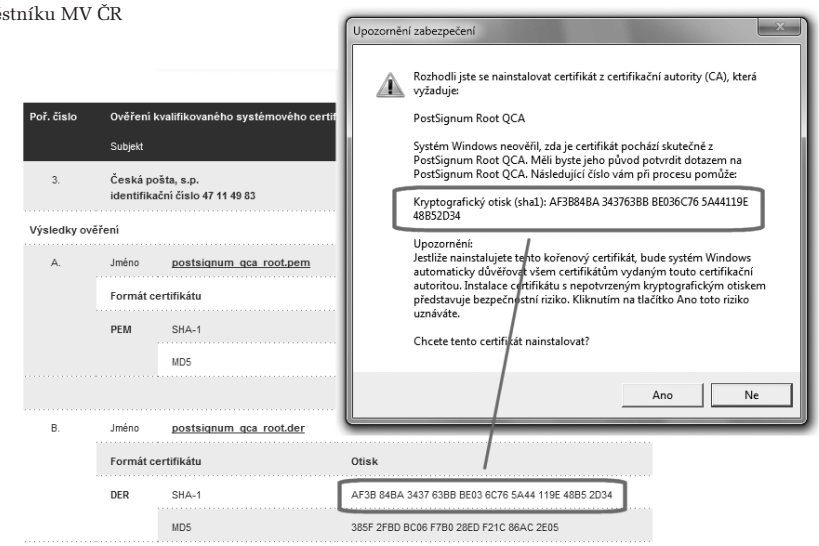
Obrázek 5-43
Příklad využití průvodce přidáním certifikátu (do systémového úložiště MS Windows)

Tento průvodce nabízí, že za uživatele sám vybere správnou složku v rámci systémového úložiště.

Ne vždy ale funguje správně, konkrétně při přidávání kořenových certifikátů certifikačních autorit, které někdy chybně přidává do složky pro certifikáty zprostředkujících autorit. Proto je vhodnější raději vybrat příslušnou složku explicitně, jako na předchozí ukázce.

V případě, kdy je přidáván nový kořenový certifikát certifikační autority (do složky pro kořenové certifikáty důvěryhodných certifikačních autorit), je na samotném konci průvodce – a ještě před skutečným vložením nového kořenového certifikátu – uživatel požádán o souhlas s vložením certifikátu. Přitom je mu zobrazen otisk nově vkládaného certifikátu a očekává se, že hodnotu tohoto otisku ověří. Viz následující obrázek.

Obrázek 5-44
Ověření otisku (původního) certifikátu CA PostSignum (PostSignum Root QCA) oproti hodnotě, uvedené ve věstníku MV ČR



5.5 Správa vlastních certifikátů

Vlastní certifikáty se od certifikátů třetích stran liší ve dvou zásadních aspektech. Prvním z nich je účel, kterému slouží: certifikáty třetích stran používáme při vyhodnocování platnosti „cizích“ elektronických podpisů, značek či časových razítek. Naproti tomu vlastní certifikáty nám umožňují vytvářet naše vlastní elektronické podpisy.

Dalším zásadním rozdílem je držení soukromého klíče: vlastní certifikáty jsou nám užitečné pouze tehdy, pokud k nim máme odpovídající soukromý klíč. Naopak od certifikátu třetí strany soukromý klíč nemáme a mít ani nemůžeme (protože nám ho ona třetí strana nesmí dát).

Z těchto zásadních rozdílů pak vyplývají i odlišnosti ve správě vlastních certifikátů a certifikátů třetích stran. Na jednu z těchto odlišností jsme přitom již narazili, v úvodu této kapitoly: certifikáty třetích stran, které jsou plně veřejné, nemusíme chránit proti okopírování (zajišťovat jejich důvěrnost). A tak si je můžeme uchovávat v kterémkoli úložišti. Obvykle v tom, jehož používání je pro nás nejjednodušší.

Naproti tomu vlastní certifikáty, pokud je chceme využít pro vytváření vlastních podpisů, musíme uchovávat spolu s odpovídajícími soukromými klíči. A to znamená zajistit, aby si náš soukromý klíč nemohl nikdo okopírovat. Stejně tak bychom ale měli požadovat i spolehlivost a dostupnost uložení soukromého klíče (spolu s certifikátem), tak abychom o něj nepřišli a mohli jej využívat. Třeba i po přechodu na nový počítač, po havárii pevného disku atd.

V praxi by to mělo být tak, že své vlastní certifikáty (a jim odpovídající soukromé klíče) si uchováváme nejlépe na externích úložištích typu čipových karet či USB tokenů. Po technické stránce je samozřejmě možné je uchovávat i v interních úložištích, jako například v systémovém úložišti operačního systému MS Windows. Je to asi nejjednodušší, a také nejlevnější řešení. Z hlediska bezpečnosti by to ale mělo být jen nouzovým řešením. Stejně tak z ryze praktického hlediska: když nám například zhavaruje pevný disk, přijdeme o certifikáty a soukromé klíče, uložené v systémovém úložišti.

Pojďme si nyní podrobněji rozebrat postup při získávání nového (osobního) certifikátu.

5.5.1 Co je třeba vědět, než budete žádat o vydání certifikátu?

Certifikát, který si chceme pořídit, nám bude vystavovat nějaká certifikační autorita. Tu si sice můžeme provozovat i sami, na vlastním počítači – ale zde raději předpokládejme, že o vystavení certifikátu požádáme nějakou etablovanou a důvěryhodnou certifikační autoritu. Pokud chceme získat certifikát kvalifikovaný, stejně se musíme obrátit na některou kvalifikovanou certifikační autoritou. Což v ČR znamená některou z akreditovaných, protože všechny kvalifikované jsou současně i akreditovanými.

Než ale půjdeme za jakoukoli certifikační autoritou, měli bychom mít na paměti jedno základní pravidlo (byť z něj existují určité výjimky, viz dále): že tzv. párová data, neboli soukromý a veřejný klíč, si nejprve musíme vygenerovat sami – a teprve pak můžeme jít za certifikační autoritou (s příslušnou žádostí) a chtít po ní, aby nám k těmto párovým datům vystavila požadovaný certifikát.

Důvodem je bezpečnost: pokud by náš soukromý klíč vytvořil někdo jiný a pak nám ho předal, měli bychom skutečně jistotu, že si ho předtím nezkopíroval či jinak neschoval jeho kopii? Pokud by tak učinil, mohl by se platně podepisovat naším jménem.

S tím úzce souvisí i další nesmírně důležitá skutečnost, kterou si také musíme uvědomit: poté, co si svá nová párová data (soukromý a veřejný klíč) vygenerujeme sami, certifikační autoritě předáme

(v rámci žádosti o nový certifikát) pouze svůj veřejný klíč. Svůj soukromý klíč jí nepředáváme, ani jinak nesdělujeme jeho hodnotu!

Jak nám pak ale může jakákoli certifikační autorita vystavit jakýkoli certifikát, když se nedostane k našemu soukromému klíč?

Připomeňme si, že každý certifikát obsahuje veřejný klíč a údaje o identitě konkrétní osoby, a že vydavatel certifikátu osvědčuje, že dotyčná osoba má ve svém držení příslušný soukromý klíč (tj. ten, který je „do páru" s veřejným klíčem, obsaženým v certifikátu). Jak se ale certifikační autorita při vydávání certifikátu může přesvědčit, že skutečně máme odpovídající soukromý klíč, když jí ho nehodláme dát (ani ukázat, resp. sdělit jeho hodnotu)?

Odpověď je naštěstí principiálně jednoduchá: díky možnostem asymetrické kryptografie můžeme certifikační autoritě prokázat, že soukromý klíč máme, aniž bychom ho dali z ruky. Stačí nám využít stejné principy asymetrické kryptografie, o které se opírá samotný elektronický podpis a které jsme si popisovali již v části 1.8: co je „uzamčeno" (podepsáno) pomocí soukromého klíče, lze „odemknout" (ověřit) právě a pouze odpovídajícím veřejným klíčem.

Takže když žádáme o vystavení certifikátu, v rámci své žádosti musíme něco „zamknout" soukromým klíčem. Třeba právě samotnou žádost o vydání nového certifikátu.[17] K té přiložíme odpovídající veřejný klíč a vše předáme certifikační autoritě. Ta si ověří, že „zamknutý" obsah lze odemknout předloženým veřejným klíčem – a právě tím získává jistotu, že žadatel má v ruce odpovídající soukromý klíč.

5.5.1.1 Kde generovat párová data?

Jak jsme si již několikrát zdůraznili, kvůli bezpečnosti (ale i z ryze praktických důvodů) je vhodné si své osobní certifikáty, spolu s odpovídajícími soukromými klíči, uchovávat na externích úložištích typu čipových karet či USB tokenů. To ale souvisí i s jejich generováním, protože již samotný způsob počátečního vygenerování párových dat (soukromého a veřejného klíče) může předurčovat možnost jejich uložení a následného praktického používání.

Berme jako obecné pravidlo (s možností určitých výjimek), že když svůj soukromý klíč vytvoříme v nějakém konkrétním úložišti, ať již jde o interní softwarové úložiště či externí úložiště typu čipové karty nebo USB tokenu, nemůžeme s tímto soukromým klíčem již později „hýbat" a přemisťovat ho do jiného úložiště.

Což znamená i to, že když si k tomuto soukromému klíči necháme vystavit osobní certifikát, můžeme tento certifikát následně uložit právě a pouze na to samé místo (do toho samého úložiště), ve kterém se nachází soukromý klíč.

---

[17] Zde se jedná o žádost ve smyslu věcném, resp. technickém, která má podobu souboru (obvykle s příponou .req).

Uvedené pravidlo je dokonce ještě přísnější v tom smyslu, že se netýká jen úložišť certifikátů jako takových, ale dokonce i jednotlivých modulů CSP (Certificate Services Provider, viz část 5.1.3.1): když si svá párová data (soukromý a veřejný klíč) necháme vygenerovat pomocí konkrétního modulu CSP v konkrétním úložišti, můžeme následně vydaný certifikát uložit do stejného úložiště pouze prostřednictvím toho samého modulu CSP. Důvodem je to, že již samotný modul CSP předurčuje takové parametry, jako je velikost klíčů či používaná hašovací funkce atd.

Pamatujme na právě popsané skutečnosti už i kvůli tomu, že z nich vyplývá jeden nesmírně důležitý závěr:

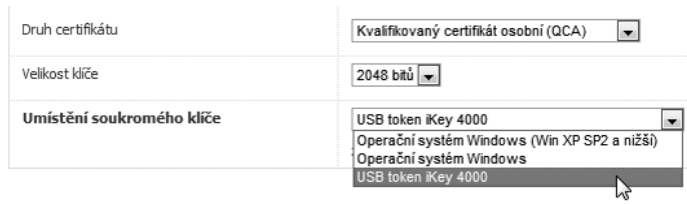
Na to, kde chceme uchovávat svůj osobní certifikát i s odpovídajícím soukromým klíčem, musíme pamatovat ještě před žádostí o vystavení certifikátu, a to místem a způsobem generování párových dat (soukromého a veřejného klíče).

V praxi se bohužel často stává, že uživatelé si připraví žádost o vydání nového certifikátu (a v rámci ní si nechají vygenerovat i nová párová data) na jednom počítači – a když jim certifikační autorita vydá požadovaný certifikát, chtějí si ho nainstalovat někam jinam, na jiný počítač. Což se jim ale nepodaří.

Stejný problém nastává i v situaci, kdy se vše odehrává na stejném počítači, ale využita mají být různá úložiště: například když v rámci generování žádosti o vydání nového certifikátu jsou nová párová data vytvořena v systémovém úložišti MS Windows, ale uživatel by si chtěl uložit svůj certifikát (i s odpovídajícím soukromým klíčem) na čipovou kartu či USB token.

Mějme tedy stále na paměti, že na budoucí uložení soukromého klíče (a tím i možnost uložení osobního certifikátu k tomuto klíči) musíme pamatovat již při generování žádosti o vystavení certifikátu.

Jak uvidíme záhy, při vytváření žádosti o nový certifikát na to je snad vždy pamatováno tak, aby si žádající uživatel mohl vybrat příslušné úložiště (i modul CSP). Prozatím si to naznačme alespoň následujícím obrázkem, než se ke generování žádostí dostaneme znovu a podrobněji.



Obrázek 5-45
Volba úložiště ze systémem doporučených možností

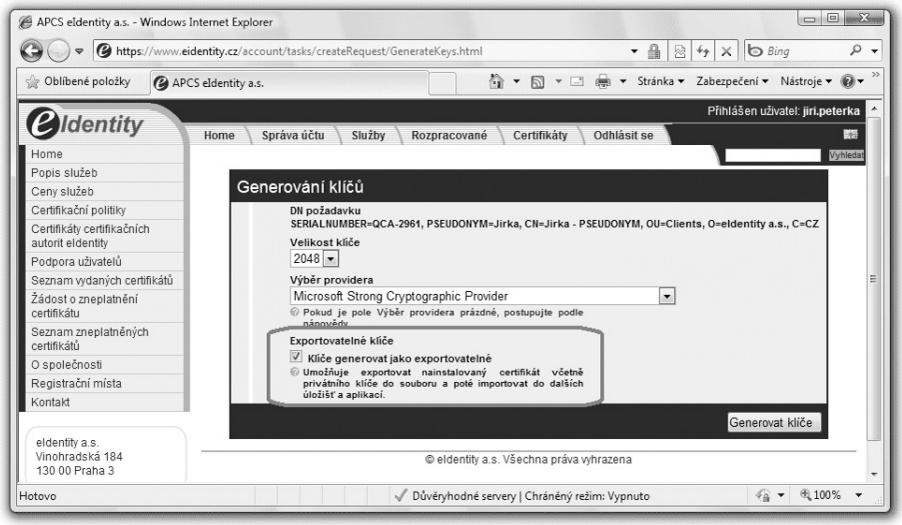
5.5.1.2 Možnost exportu soukromého klíče

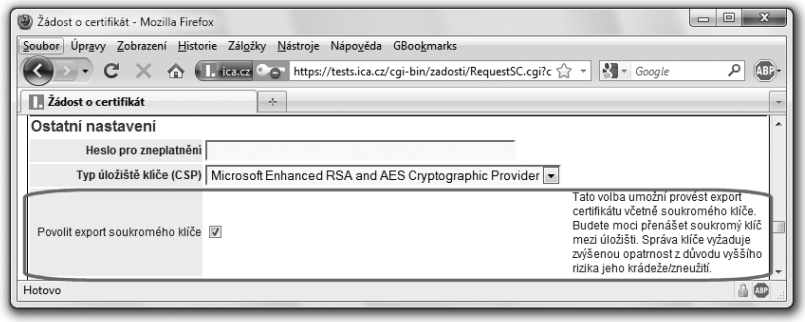
Z obecných pravidel (o vazbě soukromého klíče na konkrétní úložiště), popisovaných v předchozí části, naštěstí existují určité výjimky. Konkrétně možnost tzv. **exportu soukromého klíče.** Ta se ale netýká „počáteční fáze“ žádosti o certifikát a nezbavuje nás nutnosti instalovat nově vydaný certifikát přesně

do toho úložiště, do kterého byl vygenerován soukromý klíč. Možnost exportu se týká až následného postupu: když už jsme nový certifikát nainstalovali „tam, kde jsme vytvářeli žádost“ a kde se nachází odpovídající soukromý klíč, umožňuje nám následně provést „export“ tohoto certifikátu i se soukromým klíčem do námi zvoleného souboru. Tento soubor pak můžeme nějak zálohovat, ale stejně tak můžeme jeho obsah „importovat“ do jiného úložiště.[18] A tím dosáhnout „přenesení“ osobního certifikátu, spolu s odpovídajícím soukromým klíčem, do jiného úložiště.

Obrázek 5-46

Příklady volby (prováděné již při žádosti o nový certifikát), zda soukromý klíč má být exportovatelný





18 Ovšem pouze do takového úložiště (a skrze takový modul CSP), který je kompatibilní s původním úložištěm (a modulem CSP), například co do rozsahu klíčů a používané hašovací funkce.

Upřesněme si ale, že o možnosti exportu soukromého klíče se také rozhoduje již v okamžiku generování příslušných párových dat, v rámci žádosti o vydání nového certifikátu. Takže, řečeno jinými slovy: chceme-li (později) mít možnost exportu soukromého klíče, musíme na to pamatovat již na počátku, při vytváření příslušné žádosti o vydání nového certifikátu, a příslušný soukromý klíč nechat generovat rovnou jako **exportovatelný**.

Stejně tak ale mějme na paměti, že ne vždy je to možné. V řadě případů, kdy dochází ke generování párových dat, není možné nastavení „exportovatelnosti" soukromého klíče ovlivnit.

Například pokud žádáte o vydání nového osobního certifikátu u CA PostSignum, je klíč generován jako exportovatelný automaticky a žadatel nemá možnost toto změnit. V případě I. CA a eIDentity máte možnost si sami zvolit, zda má být soukromý klíč generován jako exportovatelný či nikoli, viz předchozí dva obrázky.

5.5.1.3 Generování soukromého klíče přímo v čipové kartě či tokenu

Jiným příkladem toho, kdy možnost exportu soukromého klíče nemůžeme ovlivnit, jsou právě externí úložiště charakteru čipových karet a USB tokenů.

Ty dnes umožňují generovat nová párová data (nový soukromý a veřejný klíč) přímo uvnitř karty či tokenu, ale z důvodu vyšší bezpečnosti (kvůli které jsou používány) ani nepřipouští možnost jakéhokoli exportu soukromého klíče. Takže ten ani není možné generovat jako exportovatelný.

S touto vlastností čipových karet a USB tokenů souvisí i výjimka z dříve popisovaného pravidla: že od certifikační autority bychom neměli nikdy požadovat, aby nám generovala naše párová data (ale měli bychom si je vždy generovat sami a svůj soukromý klíč nedávat nikomu, ani certifikační autoritě).

V případě čipových karet a USB tokenů však lze udělat výjimku: jelikož zde nehrozí, že by certifikační autorita mohla soukromý klíč nějak „vytáhnout ven" z karty či tokenu, může po ní chtít, aby nám vygenerovala naše párová data ona.

Jinými slovy: pouze v tomto případě, kdy nám certifikační autorita poskytuje i kartu či token, nemusíme svá párová data generovat sami a můžeme to požadovat od certifikační autority.[19]

---

[19] Alespoň teoreticky je ale možné, aby certifikační autorita generovala párová data pro svého zákazníka i v jiných případech, kdy nejde o čipovou kartu či token. Pamatuje na to zákon (č. 227/2000 Sb., o elektronickém podpisu), který ale v takovém případě autoritu zavazuje k přísným bezpečnostním opatřením (požaduje utajení klíčů před jejich předáním, zakazuje jejich kopírování a uchovávání déle, než je nezbytné). Tuzemské certifikační autority této možnosti ale v praxi většinou nevyužívají.

5.5.1.4 Ověření identity žadatele

Další důležitý úkon, který musí certifikační autorita udělat, je zjistit a ověřit si identitu žadatele.[20] To proto, aby přesně věděla, komu svůj certifikát vystavuje. Dále proto, aby věděla, co má uvést do kolonky pro držitele certifikátu (formou jména DN, Distinguished Name).[21]

> Připomeňme si, v souvislosti s částí 4.9, že mezi „úplností" informací v držení certifikační autority a hodnotou řetězce DN, obsaženého přímo v certifikátu, může být významný rozdíl. Informace, které certifikační autorita získává, musí postačovat k jednoznačné identifikaci osoby, které byl certifikát vystaven. Hodnota řetězce DN k tomu stačit nemusí.

Pokud tedy žádáte nějakou certifikační autoritu o vystavení certifikátu poprvé, budete se muset k ní dostavit osobně a prokázat se tolika doklady, kolik jich po vás bude požadovat. Obvykle jde o občanský průkaz a jeden další doklad, jako například pas, řidičský průkaz apod.

V praxi přitom nemusíte vždy chodit jen na centrálu příslušné certifikační autority, která může být někde daleko od vás. Můžete navštívit i některou z tzv. **registračních autorit**, se kterými certifikační autority spolupracují právě na přesné identifikaci žadatelů o vystavení. Může to být třeba i nějaký obecní či městský úřad apod. Princip je ale stále stejný: je nutná osobní návštěva a ověření identity přes „fyzické" doklady totožnosti.

Jinak tomu může být v případě, kdy již nějaký certifikát máte a chcete požádat stejnou certifikační autoritu o vystavení nového certifikátu. V takovém případě vás certifikační autorita již zná a na novém „fyzickém kontaktu" již nemusí trvat. Může jí stačit, když svou žádost o nový certifikát opatříte svým elektronickým podpisem, založeným na dosavadním certifikátu. Samozřejmě za předpokladu, že tento certifikát ještě platí.

5.5.1.5 Obnova certifikátů

Připomeňme si také, že certifikáty se zásadně neprodlužují. Není to možné již jen kvůli tomu, že mají od začátku pevně nastavenou dobu řádné platnosti. A ta může být pouze předčasně zkrácena, skrze revokaci.

Místo prodloužení platnosti dosavadního certifikátu se vždy vystavuje certifikát nový.

Někdy se o takovémto certifikátu hovoří jako o certifikátu návazném či následném. Jindy se zase mluví o obnově původního certifikátu či o obnoveném certifikátu, i když toto je dosti zavádějící: obnova by

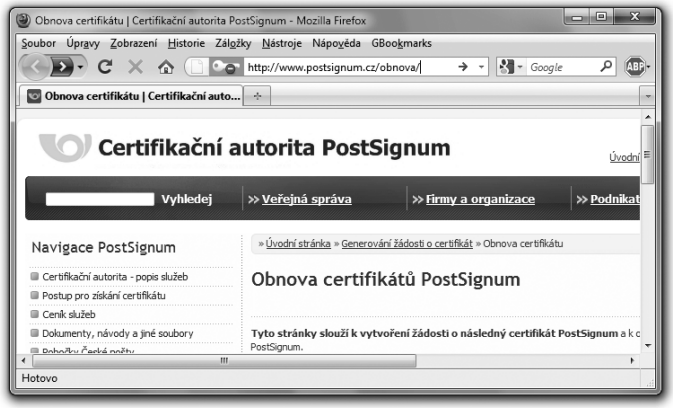
---

20 Zde předpokládáme pouze situaci, kdy o vydání certifikátu žádá přímo ta osoba, které (a na jejíž jméno) bude certifikát následně vystaven. Neuvažujeme zde případ tzv. zaměstnaneckých certifikátů, o jejichž vystavení pro konkrétní zaměstnance může žádat pověřený zástupce organizace (tzv. pověřená osoba).

21 Toto samozřejmě neplatí pro takové druhy certifikátů, jako jsou testovací či emailové apod. Obecně ty, které negarantují, komu byl certifikát vystaven.

totiž mohla implikovat nějaké „vzkříšení“ původního certifikátu a prodloužení (obnovu) jeho životnosti. A to rozhodně není možné. Vždy se vystavuje nový certifikát.

Obrázek 5-47
Nabídka „Obnovy certifikátů“ na stránkách CA PostSignum je ve skutečnosti nabídkou na vystavení zcela nového (následného) certifikátu



5.5.2 Žádost o vydání nového certifikátu

Z výše uvedených skutečností vyplývá, že kromě případu s čipovou kartou či USB tokenem[22] by zájemce o vydání certifikátu neměl „jen tak“ přijít na certifikační (či registrační) autoritu a požadovat po ní, aby mu certifikát vystavila. Přesněji neměl by chtít, aby vše začalo až teprve na certifikační autoritě.

Místo toho je nutné, aby si zájemce o certifikát nejprve připravil – a to „u sebe“, na svém počítači – potřebnou **žádost o vydání nového certifikátu**. Přílohou takovéto žádosti nejspíše budou i určité smluvní dokumenty, které musí žadatel vyplnit. Samotnou žádostí (ve věcném slova smyslu) je ale datový soubor předepsaného formátu (PKCS#10, viz část 5.3.2.), obvykle s příponou .req.

> Jak již víme z předchozího výkladu, ještě před touto žádostí (nebo v rámci jejího vytváření) muselo dojít ke generování nezbytných párových dat tak, aby veřejný klíč mohl být přiložen k samotné žádosti, a tato mohla být podepsána pomocí odpovídajícího soukromého klíče.

Teprve se správně vytvořenou žádostí má smysl chodit na certifikační autoritu a chtít po ní vystavení nového certifikátu. Případně jej certifikační autoritě poslat, pokud pro vydání certifikátu není nutná osobní přítomnost žadatele (viz dále). Protože to první, co certifikační autorita bude po každém žadateli požadovat, je právě takováto (správně vytvořená) žádost.

Připomeňme si také, že již při generování žádosti musí zájemce správně zohlednit to, jak bude chtít následně vydaný certifikát používat, především pokud jde o jeho uložení a možnost exportu. Musí na to pamatovat již při generování párových dat, které pro svou žádost potřebuje.

[22] Kdy certifikační autorita poskytne zákazníkovi novou kartu či token, a párová data generuje přímo v této kartě či tokenu.

Snad netřeba zdůrazňovat, že certifikační autorita neodpovídá za případné chyby, ke kterým zde může dojít. Například pokud si uživatel nechá vygenerovat soukromý klíč jako neexportovatelný, a kvůli tomu nejde exportovat a následně importovat do jiného úložiště, není to vina certifikační autority a není to důvodem k bezplatnému vydání nového certifikátu. Obdobně v případě, kdy si uživatel nechal vygenerovat soukromý klíč do nějakého konkrétního úložiště, ale pak o něj přišel (například kvůli havárii disku). Nebo když potřebuje instalovat již vydaný certifikát do jiného úložiště (či jen skrze jiný CSP modul), než do kterého byl vygenerován soukromý klíč.

5.5.2.1 Možnosti generování žádostí o vydání certifikátu

Samotné generování žádosti o nový certifikát (ve výše popsaném smyslu) může být realizováno různými způsoby, které mohou být různě uživatelsky vstřícné. Stejně tak mohou být jednotlivé způsoby více či méně vhodné podle toho, kolik takovýchto žádostí je generováno a jak často. Protože něco jiného se hodí pro jednotlivce, který žádá o nový certifikát (pro sebe sama) jednou za rok, a něco jiného zase pro specialistu ve firmě, který generuje velké počty žádostí o zaměstnanecké certifikáty.

Zde si proto popíšeme dvě varianty generování žádostí, které jsou v praxi asi nejčastější a týkají se spíše příležitostného (než nějakého „sériového“) generování žádostí.

První varianta, označovaná také přívlastkem „on-line“, spočívá v generování žádosti přímo pomocí běžného prohlížeče. Pro jednorázové použití koncovým uživatelem bývá nejjednodušší. Pro opakované, resp. častější generování žádostí je zase vhodnější druhá varianta, označovaná přívlastkem „off-line“ a využívající specializovanou aplikaci spouštěnou přímo na uživatelově počítači. Ta je řešením i pro takového uživatele, který potřebuje jen jednorázově vygenerovat svou žádost, ale jeho prohlížeč nesplňuje požadavky, které na něj klade zvolená certifikační autorita.

5.5.2.2 Generování žádosti on-line způsobem

Varianta generování žádosti on-line způsobem (tj. prostřednictvím webového prohlížeče) vždy vyžaduje, aby prohlížeč považoval příslušnou certifikační autoritu a její webové stránky za důvěryhodné.

Je to nutné proto, aby prohlížeč byl ochoten provést úkony, které po něm tyto stránky požadují. Z pohledu uživatele to sice může vypadat tak, že generování žádosti (a v rámci ní i generování párových dat, tedy soukromého a veřejného klíče) probíhá „na stránkách certifikační autority“, ve skutečnosti je tomu ale jinak – ke generování párových dat dochází na počítači uživatele, a párová data (soukromý a veřejný klíč) jsou vytvářena v tom úložišti a prostřednictvím toho modulu CSP, který si uživatel určí.

Aby ale něco takového bylo možné, musí si webové stránky certifikační autority vyžádat spuštění určitého kódu („kusu programu“) v rámci uživatelova prohlížeče. Tento kód pak aktivně zasahuje do místního počítače (generuje párová data v příslušném úložišti certifikátů). Proto prohlížeč musí mít jistotu, že požadavek na spuštění onoho „kusu programu“ je legitimní a může mu vyhovět.

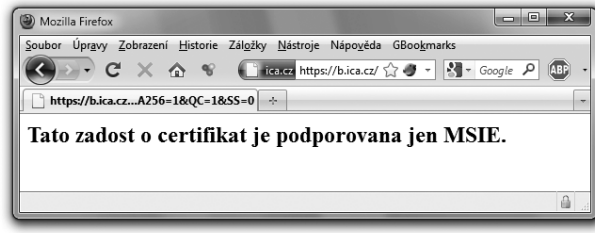
V praxi to vyžaduje, aby kořenové certifikáty příslušné certifikační autority (a raději i certifikáty všech podřízených, resp. zprostředkujících autorit) byly nainstalovány v příslušných složkách toho úložiště, se kterým používaný prohlížeč pracuje, a ten je kvůli tomu považoval za důvěryhodné. Díky tomu pak bude považovat za důvěryhodný i serverový certifikát, kterým se prokazují webové stránky certifikační autority, a také certifikát, na kterém je založen podpis toho kódu („kusu programu“), který má být na počítači žadatele spuštěn.

Někdy ale může být zapotřebí i to, aby za důvěryhodné byly explicitně prohlášeny i URL adresy konkrétních webových serverů certifikační autority, viz obrázek.

Obrázek 5-48
Přidání webu CA PostSignum mezi důvěryhodné v Internet Exploreru

Řekněme si rovnou, že snad ve všech případech musí jít o prohlížeč Internet Explorer na platformě MS Windows. Jiné prohlížeče obvykle nejsou certifikačními autoritami podporovány (pro generování žádostí). Připomeňme si to na již jednou uvedeném obrázku (v části 5.3).

Obrázek 5-49
Příklad on-line služby (žádosti o certifikát u I.CA), která funguje jen v Internet Exploreru



Dalším problémem, který v praxi vyvstane před uživatelem je to, že prohlížeč „neumí“ sám od sebe ty činnosti, které po něm webové stránky certifikační autority požadují, a které jsou nezbytné pro sestavení žádosti o vydání certifikátu (zejména pro generování klíčů a elektronické podepsání žádosti). Jinými slovy: webové stránky s on-line žádostí potřebují spustit určitý kód („kus programu“), který ale není v rámci webového prohlížeče k dispozici. A tak je nutné jej alespoň dodatečně doinstalovat, ve formě vhodného modulu plug-in či prvku ActiveX.

> I zde si můžeme říci, že je běžnou praxí, aby různé certifikační autority vyžadovaly instalaci různých knihoven (resp. různých modulů či prvků ActiveX apod.).

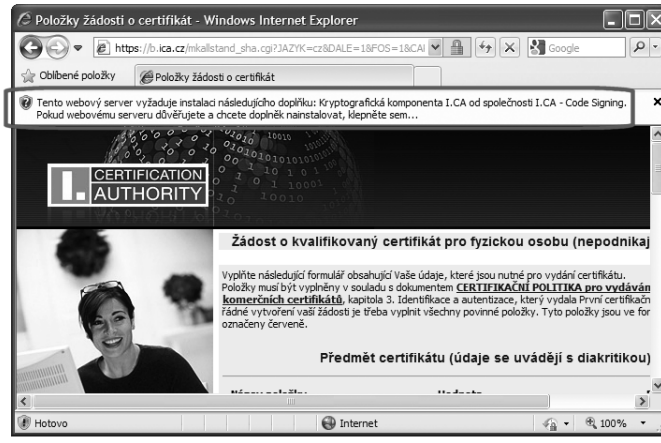
Podrobněji jsme si tuto problematiku popisovali v části 5.2.2, a tak si jen připomeňme, na již jednou uvedených obrázcích, že pro generování žádosti o certifikát od CA PostSignum je požadována instalace ActiveX prvku „Microsoft Certificate Enrollment Control“, zatímco u I.CA je požadována instalace ActiveX prvku I.CA – Code Signing.

Obrázek 5-50

Příklad žádosti o instalaci prvku ActiveX

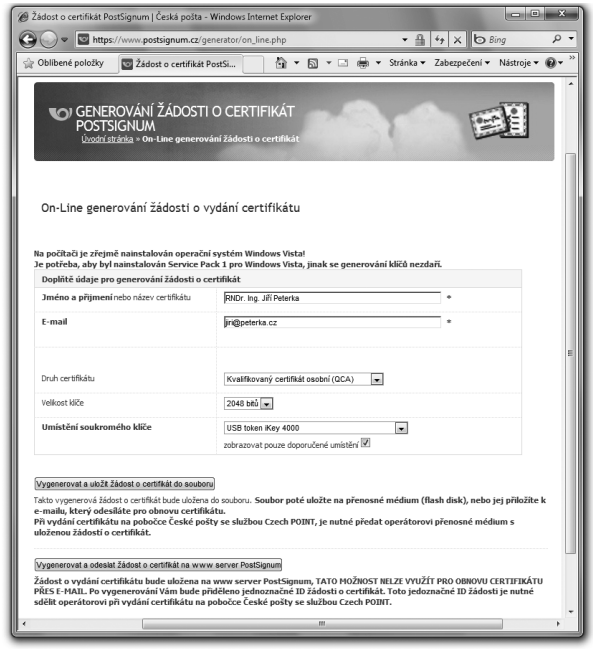
Obrázek 5-51

Příklad instalace vlastní knihovny od I.CA



Když už se podaří generování žádosti o vystavení certifikátu v prohlížeči spustit, může být její vyplnění již relativně jednoduché. Například u žádosti o vystavení osobního kvalifikovaného certifikátu pro nepodnikající fyzickou osobu u CA PostSignum (viz obrázek na předchozí stránce) žadatel zadává jen své jméno, příjmení a emailovou adresu.[23]

Obrázek 5-52
Příklad formuláře s žádostí o vystavení nového certifikátu u CA PostSignum

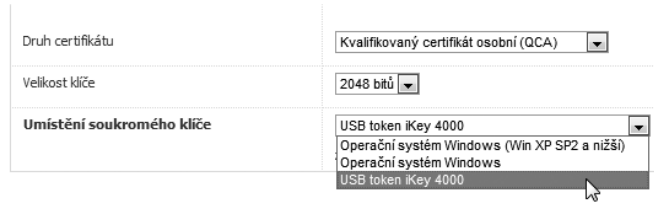


Pozor musíme dát na to, jak velký klíč chceme generovat (dnes již jde standardně o klíče velikosti 2048 bitů), a pak hlavně na volbu správného úložiště. Na předchozím obrázku (u CA PostSignum) je tato volba označena jako volba „umístění soukromého klíče“, ale ve skutečnosti je něčím více, než jen volbou úložiště. Zahrnuje totiž i volbu poskytovatele kryptografických služeb (modulu CSP), prostřednictvím kterého má dojít k vygenerování soukromého (a veřejného) klíče v příslušném úložišti.

Nabídka „umístění soukromého klíče“ se přitom může lišit podle toho, zda na svém počítači máme nainstalováno (a momentálně i dostupné) nějaké externí úložiště, v podobě čipové karty či USB tokenu. Předchozí obrázek byl snímán na počítači, kde byl dostupný právě USB token iKey 4000 – a tak formulář žádosti sám od sebe nabídl umístění soukromého klíče na tento token jako první (a tím i doporučenou) možnost. Vedle ní je nabízeno ještě systémové úložiště operačního systému MS Windows, viz následující obrázek (ve dvou verzích, lišících se podle kompatibility se staršími verzemi operačního systému MS Windows).

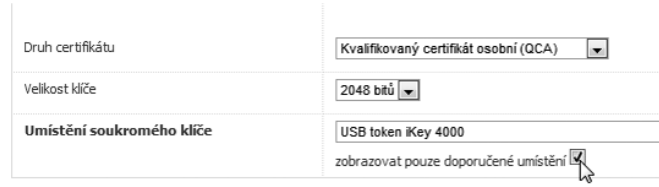
[23] Emailová adresa je u CA PostSignum povinná, ale jinde (například u eIdentity) povinná není.

Obrázek 5-53
Volba úložiště ze systémem doporučených možností



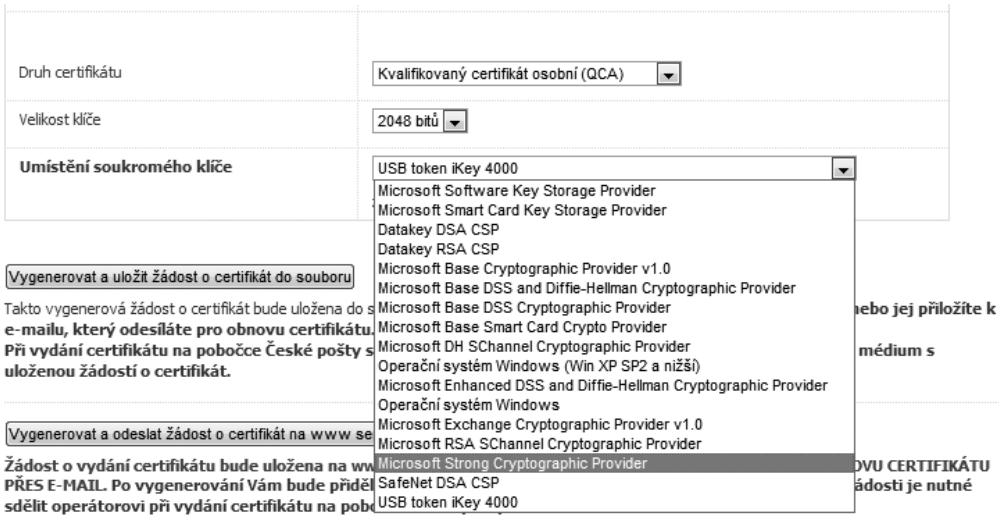
Zkušenější uživatelé si mohou zvolit ještě řadu dalších poskytovatelů kryptografických služeb (modulů CSP). Nejprve je ale třeba zrušit omezení jen na doporučená umístění:

Obrázek 5-54
Zrušení omezení jen na doporučená umístění



Pak je možných umístění (poskytovatelů kryptografických služeb) nabídnuto podstatně více.

Obrázek 5-55
Nabídka dalších podporovaných úložišť



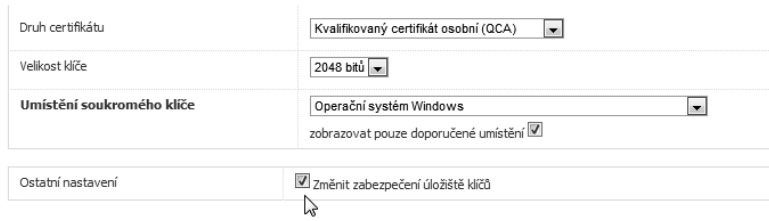
Připomeňme si také, že již při generování žádosti o vystavení certifikátu (u CA PostSignum) se rozhoduje i o možnosti exportu („exportovatelnosti“) soukromého klíče. I tato volba je ale závislá na tom, jaké úložiště je pro generování párových dat zvoleno (a jaký poskytovatel, resp. modul CSP): u externích úložišť typu čipových karet a USB tokenů je soukromý klíč generován rovnou jako neexportovatelný, a uživatel nemá možnost to změnit.

U ostatních úložišť (která jsou interní a řešená softwarově) již možnost volby poskytnuta být může. Ale, jak již víme, například u žádostí o certifikát od CA PostSignum poskytnuta není, a soukromý klíč je v těchto úložištích vždy generován jako exportovatelný.

S generováním párových dat a uložením soukromého klíče ve vnitřním softwarovém úložišti (například v systémovém úložišti MS Windows) ale souvisí ještě jedna důležitá volba: toho, jak moc má být v tomto úložišti soukromý klíč chráněn. Nejčastěji jde o to, že přístup k soukromému klíči může být chráněn ještě heslem – a pak lze nastavit, kdy (a jak často) se toto heslo musí zadávat.

> V případě systémového úložiště MS Windows je soukromý klíč chráněn nejvíce, pokud každé jeho použití vyžaduje zadání správného hesla. To je nejvyšším stupněm ochrany, kterou systémové úložiště v MS Windows nabízí. Nižším (prostředním) stupněm je nutnost potvrdit každé použití soukromého klíče (prostým kliknutím, nikoli zadáním hesla). Při nejnižším stupni ochrany soukromého klíče není jeho použití uživateli ani signalizováno, natož aby byl požadován jeho souhlas.

Nejprve tedy musíme zvolit umístění certifikátu do systémového úložiště. Díky tomu nám formulář nabídne možnost „Změnit zabezpečení úložiště klíčů“, kterou musíme zaškrtnut, viz následující obrázek.

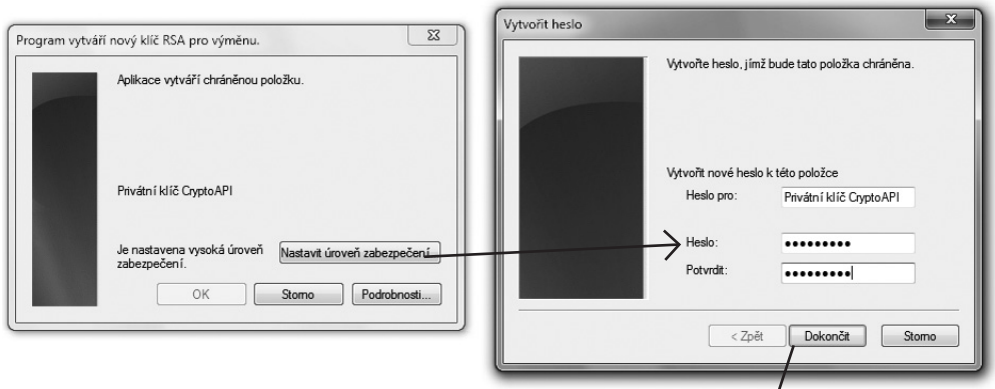


Obrázek 5-56
Volba změny zabezpečení

> Možnost změnit zabezpečení je pak skutečně nabídnuta až v okamžiku, kdy je zahájeno generování klíčů. Pak se objeví nabídka pro volbu nejvyšší úrovně ochrany, která vyžaduje zadání hesla, viz obrázek.

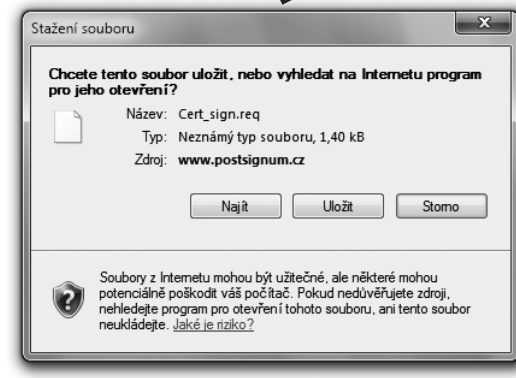
Obrázek 5-57

Volba vysoké úrovně ochrany a zadání hesla



Obrázek 5-58

Uložení souboru s žádostí o vystavení certifikátu



Po úspěšném zadání hesla již může generování žádosti o nový certifikát doběhnout do konce.

To znamená, že je vytvořen soubor s příponou .req (v daném případě Cert_sign.req), který obsahuje samotnou žádost a který je třeba si vhodně uložit, například na USB flash disk – a poté odnést na certifikační autoritu jako podklad pro vystavení certifikátu.

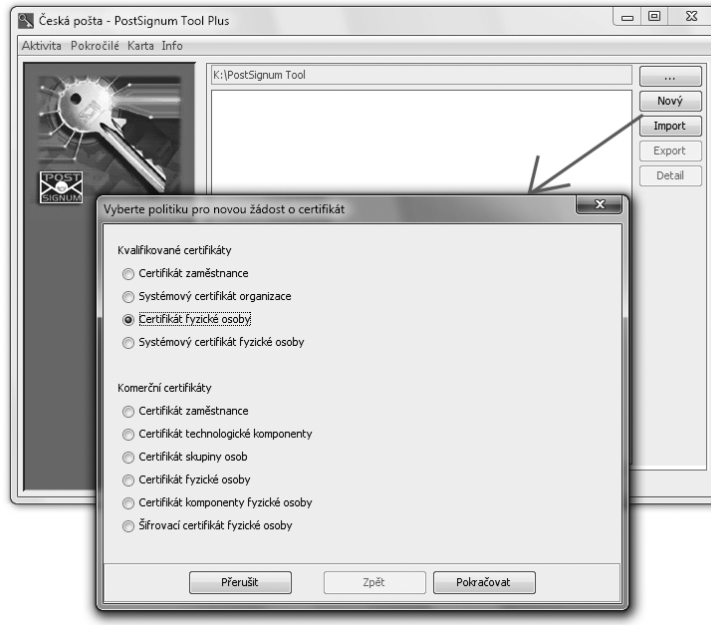
5.5.2.3 Generování žádosti off-line způsobem

Alternativou ke generování žádosti o nový certifikát přímo ve webovém prohlížeči je využití specializované aplikace, kterou uživateli poskytne certifikační autorita.

> Například u certifikační autority PostSignum jde o aplikaci s názvem PostSignum Tool. Její využití je na webu této certifikační autority prezentováno jako „off-line generování“ (na rozdíl od generování žádosti pomocí webového prohlížeče, která je označována jako „on-line generování“).

Výhodou specializované aplikace je to, že ji mohou využít i uživatelé těch prohlížečů, které nejsou certifikační autoritou podporovány (pro „on-line generování“). Stejně tak je výhodou to, že takováto specializovaná aplikace má v sobě již zabudovanou potřebnou funkčnost, a není tak nutné dodatečně instalovat různé knihovny (jako v případě generování žádosti v prohlížeči). V neposlední řadě bývá tato možnost vhodnější pro případy, kdy uživatel potřebuje generovat více žádostí, resp. generovat je častěji a ne jen příležitostně.

I pro tento způsob generování žádosti („off-line“) přitom platí to, co jsme si říkali již v souvislosti s předchozí (on-line) variantou: že již dopředu je třeba počítat s umístěním soukromého klíče a s využitím konkrétního modulu CSP.



Obrázek 5-59
Generování žádosti pomocí aplikace PostSignum Tool Plus

5.5.3 Generování žádosti o následný certifikát (obnova certifikátu)

Jak jsme si již uvedli, hovořit o obnově certifikátu – tak jak to nabízí většina certifikačních autorit – není zcela korektní. Žádný certifikát nemůže nikdy být obnoven, nebo nějak prodloužen. Jeho platnost může být pouze zkrácena, skrze předčasné zneplatnění alias revokaci. Místo prodloužení musí být vždy vydán certifikát nový.

To, co certifikační autority prezentují jako „obnovu“, je ve skutečnosti jen poněkud odlišný režim vydání nového certifikátu. Od „standardního“ režimu, který jsme si popisovali v předchozích odstavcích, se liší v jedné podstatné věci: certifikační autorita vás již „zná“ (má spolehlivě zjištěnu vaši identitu). Takže již vás nepotřebuje identifikovat znovu. Místo toho jí stačí, když se v žádosti o nový certifikát „odkážete“ na svůj dosavadní certifikát, podle kterého vás certifikační autorita pozná. Do nového certifikátu pak vloží stejné údaje (o identitě držitele), jako u stávajícího certifikátu.

> To, že „obnova certifikátu“ není ve skutečnosti žádnou obnovou původního certifikátu, natož pak nějakým jeho prodloužením, lze dokumentovat i na skutečnosti, že „obnovit“ jeden původní certifikát lze vícekrát (tolikrát, kolikrát jen držitel chce). Pokaždé je přitom žádáno o vytvoření jiného nového certifikátu (s jiným sériovým číslem certifikátu).

Obrázek 5-60
Volba certifikátu, podle kterého má být generován následný certifikát

První krok při „obnově“ certifikátu proto spočívá ve výběru dosavadního (dosud platného) certifikátu, podle kterého vás má certifikační autorita identifikovat.

> Pamatujme si, že o „obnovu“ lze žádat jen v době, kdy je dosavadní certifikát stále ještě platný, a nebyl revokován.

Příklad, ukazující žádost o obnovu (ve skutečnosti vydání následného certifikátu) u certifikační autority PostSignum, ukazuje předchozí obrázek.

Další významnou odlišností žádosti o následný certifikát je to, že kvůli ní nemusíte jít (fyzicky) za příslušnou certifikační či registrační autoritou. Stačí, když svou žádost podepíšete svým elektronickým podpisem (založeným na dosavadním, stále ještě platném certifikátu) a pošlete do certifikační autority. Díky platnému elektronickému podpisu na vaší žádosti bude mít certifikační autorita jistotu, že žádost pochází skutečně od vás.

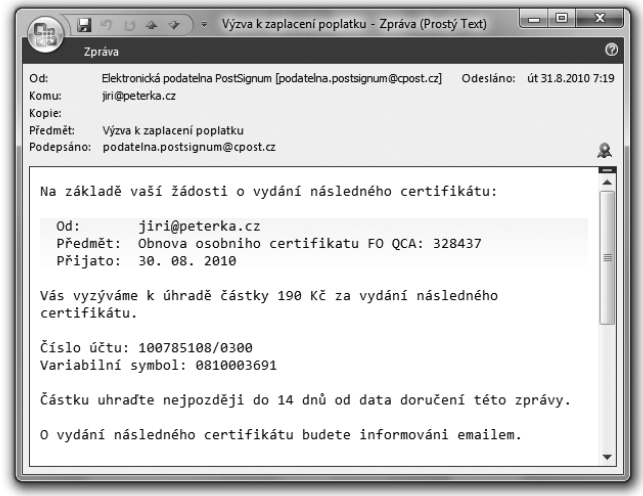
Obrázek 5-61
Nový certifikát bude zaslán emailem

A pokud za vystavení nového certifikátu zaplatíte také nějakým on-line způsobem, nemusíte za certifikační autoritou chodit už vůbec. Ona vám nový certifikát doručí také on-line způsobem.

Připomeňme si ještě, že v konkrétním případě certifikační autority PostSignum je možné generovat žádost o obnovený certifikát jak on-line způsobem, prostřednictvím prohlížeče, tak i off-line způsobem, prostřednictvím aplikace PostSignum Tool.

V prvním případě si podpis žádosti zajistí sama webová aplikace, běžící v prohlížeči uživatele. Ve druhém případě, kdy je žádost generována off-line způsobem (pomocí aplikace PostSignum Tool), ale musí žádost odeslat uživatel „ručně“. Musí ji vložit do emailové zprávy s předepsaným obsahem, a tuto žádost musí sám opatřit svým elektronickým podpisem (založeným na tom certifikátu, který má být „obnoven“).

Obrázek 5-62
Výzva k zaplacení za nový certifikát



5.5.3.1 Kdy je vhodné žádat o následný certifikát?

S „obnovováním“ certifikátů, přesněji s generováním následných certifikátů, souvisí jedna důležitá praktická otázka: jak dlouho používat stávající certifikát a kdy si jeho prostřednictvím požádat o následný certifikát?

Odpověď by na první pohled mohla být jednoduchá: stávající certifikát přeci lze používat do konce jeho řádné platnosti. Takže požádat o nový (následný) certifikát lze třeba v poslední den jeho platnosti. Stejně tak ho lze do posledního dne jeho platnosti používat i pro podepisování dokumentů v elektronické podobě.

Zatímco s první částí odpovědi (ohledně následného certifikátu) lze souhlasit, před druhou částí je třeba varovat. Pokud byste podepsali nějaký dokument těsně před koncem platnosti příslušného certifikátu, z vašeho pohledu by to ještě mohlo být v pořádku. Z pohledu příjemce takového dokumentu by tomu ale bylo jinak. Pokud by totiž nebyl podepsaný dokument opatřen ještě také časovým razítkem, pak by s koncem platnosti certifikátu (a tedy velmi brzy) skončila i možnost ověřit si platnost příslušného podpisu.

Proto tam, kde nejsou používána časová razítka (která „fixují“ v čase okamžik podpisu), je více než vhodné pamatovat i na příjemce podepsaných dokumentů a na to, kolik času jim zbude pro možnost ověření platnosti podpisu – a obnovovat právě používané certifikáty s dostatečným časovým předstihem před koncem jejich řádné platnosti.

5.5.4 Zálohování a obnova certifikátů a soukromých klíčů

S možností exportu (a následného importu) osobních certifikátů a soukromých klíčů souvisí i jejich celková správa, zahrnující jak eventuální zálohování, tak i následnou možnost obnovy. Než si ale ukážeme, jak vše v praxi funguje, je vhodné se zmínit ještě o jedné důležité věci. Tou je vhodnost a účelnost samotného zálohování „vlastních“ certifikátů (od kterých máme odpovídající soukromé klíče).

Zde je totiž velmi vhodné rozlišovat mezi kvalifikovanými certifikáty, které používáme pro vlastní podepisování, a komerčními certifikáty, které používáme pro jiné účely. Asi nejvíce specifické postavení pak mají naše komerční certifikáty, používané pro šifrování (tj. ty, které dáváme ostatním, aby je využili pro zašifrování zpráv určených nám).

Zálohování osobních kvalifikovaných certifikátů (i s odpovídajícím soukromým klíčem, je-li ten exportovatelný) je sice bezproblémové po technické stránce, ale může být velmi problematické z hlediska bezpečnosti. Pokud by se totiž někdo nepovolaný dostal k záloze, tvořené certifikátem i soukromým klíčem a dokázal ji obnovit, mohl by se platně podepisovat naším jménem (jménem držitele certifikátu).

Proto je třeba klást vysoké nároky na zabezpečení takovýchto záloh, nebo je raději ani nedělat. Ostatně, všude tam, kde soukromý klíč není exportovatelný, jako třeba u čipových karet či USB tokenů, zálohování není ani možné.

Stejně tak je třeba poměřit rizika zálohování (plynoucí z možnosti zneužití zálohy) s následky toho, že bychom o svůj kvalifikovaný certifikát i se soukromým klíčem přišli (aniž by došlo k jejich kompromitaci, tj. aniž by se dostali do rukou někomu nepovolanému). Pokud bychom si třeba svůj certifikát i se soukromým klíčem nějak nenávratně smazali (například při havárii pevného disku), škoda by nebyla nijak zásadní. Jen bychom si museli pořídit nový certifikát, kterým bychom se dále podepisovali. Naproti tomu případná kompromitace zálohovaného kvalifikovaného certifikátu i se soukromým klíčem by mohla mít mnohem nedozírnější následky: někdo jiný by se mohl platně podepisovat naším jménem (samozřejmě jen dokud bychom náš kompromitovaný certifikát nenechali revokovat).

Podobně tomu může být u komerčních certifikátů, používaných například pro přihlašování k nějakému informačnímu systému: ten, kdo by se zmocnil zálohy a dokázal náš certifikát i se soukromým klíčem použít, by se mohl vydávat za nás.

To v případě komerčních certifikátů, používaných pro potřeby šifrování, je situace přeci jen odlišná. Pokud bychom o takovýto certifikát (a hlavně o jemu odpovídající soukromý klíč) nenávratně přišli, rázem by pro nás přestaly být dostupné a čitelné všechny zprávy, které jsme přijali jako zašifrované. A to by pro nás mohlo být opravdu zásadním problémem.

Naproti tomu případná kompromitace našeho šifrovacího certifikátu a odpovídajícího soukromého klíče by umožnila někomu třetímu, aby se seznámil s tím, co mělo být určeno jen našim očím a uším. Zda by to bylo vážným problémem či nikoli, je už na individuálním posouzení každého držitele šifrovacího certifikátu: on si musí spočítat, jak velké je to které riziko, a rozhodnout, co má pro něj větší váhu.

Pojďme nyní již k tomu, jak samotné zálohování certifikátů (i se soukromými klíči) funguje.

V případě exportu certifikátu včetně soukromého klíče je výstupním formátem typicky formát PKCS#12 (viz část 5.3.2.2). V případě exportu certifikátu bez soukromého klíče bývá na výběr více možných formátů (PKCS#7, PEM, DER atd.).

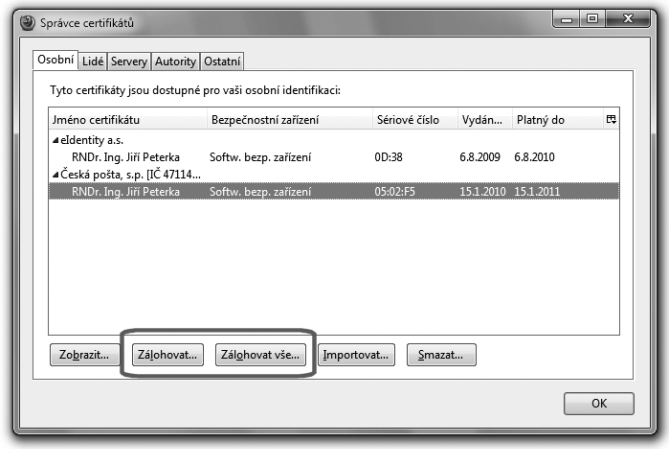
Další důležitou skutečností, kterou je třeba mít na paměti, je to, že každé úložiště certifikátů má své vlastní mechanismy jak pro import, tak i pro export certifikátů. Neexistuje tedy žádný jednotný způsob pro import a export certifikátů z/do úložišť a vždy je třeba se seznámit s tím, co a jak nabízí konkrétní úložiště certifikátů.

Naštěstí jsou standardizovány alespoň datové formáty, používané pro uchovávání certifikátů a generované či využívané při importu a exportu certifikátů (a eventuálně i klíčů), viz část 5.3. Díky tomu je možné přenášet klíče (a exportovatelné soukromé klíče) mezi jednotlivými úložišti, řešit jejich zálohování atd.

> Jednoduchým způsobem má export a import certifikátů vyřešeno úložiště certifikátů prohlížeče Mozilla Firefox. Při zobrazení každé jednotlivé složky jsou nabízeny možnosti importu přímo do této složky či možnost exportu certifikátů z této složky. Konkrétní postup při importu jsme si již podrobněji popisovali v části 5.4.4.3.

Možnost exportu je v případě složky s osobními certifikáty rovnou označována jako zálohování, a nabízena jak ve variantě zálohování jednoho konkrétního certifikátu („Zálohovat“), tak i jako zálohování všech certifikátů současně („Zálohovat vše“).

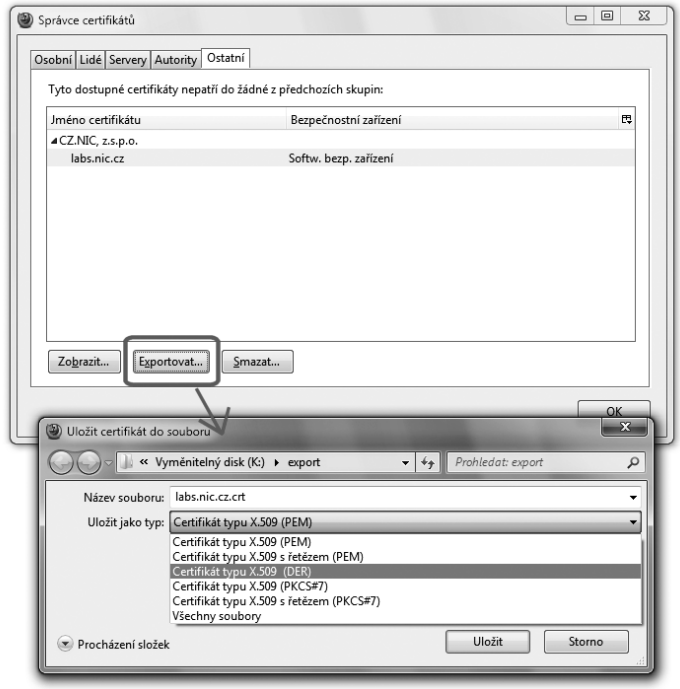
Obrázek 5-63
Možnost exportu (zálohování) certifikátů z úložiště Firefoxu



> Toto zálohování je obecně chápáno jako zálohování certifikátu spolu se soukromým klíčem, do formátu PKCS#12. Naproti tomu zálohování samotného certifikátu (bez soukromého klíče) je prohlížečem Firefox označováno jako „export“, a na výběr je hned několik výstupních formátů:

Obrázek 5-64

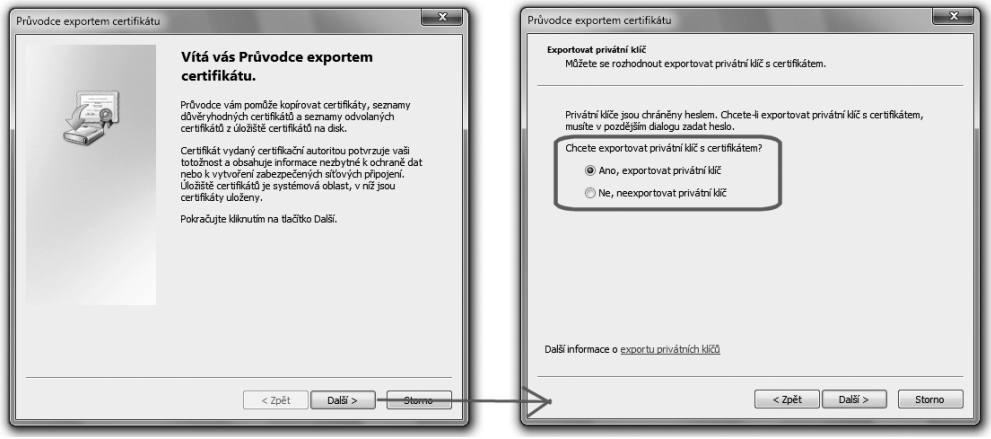
Export certifikátu v prohlížeči Firefox, bez soukromého klíče



Relativně nejpropracovanější jsou možnosti exportu a importu certifikátů z/do systémového úložiště MS Windows. Zde je pro každý z obou úkonů připraven průvodce, který uživatele provede celým úkonem.

Obrázek 5-65

Průvodce exportem certifikátu ze systémového úložiště MS Windows



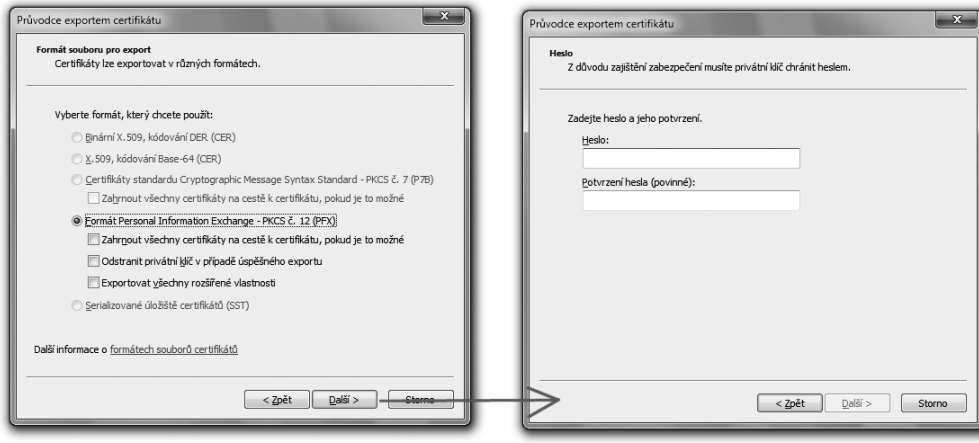
> Využití tohoto průvodce pro import (instalování certifikátů) jsme si také již ukazovali (v části 5.4.4.3), a tak si jen naznačme jeho využití pro export certifikátu.

Hned ve druhém kroku nám tento průvodce nabídne export včetně soukromého klíče či bez něj, samozřejmě v závislosti na tom, zda první varianta je vůbec možná.

V případě exportu certifikátu i se soukromým klíčem je nabídnut pouze formát PKCS#12, a uživatel je vyzván k zadání hesla. Tím bude chráněn přístup k soukromému klíči ve výstupním souboru. Stejné heslo pak bude třeba zadat při následném importu.

Obrázek 5-66

Export certifikátu spolu se soukromým klíčem



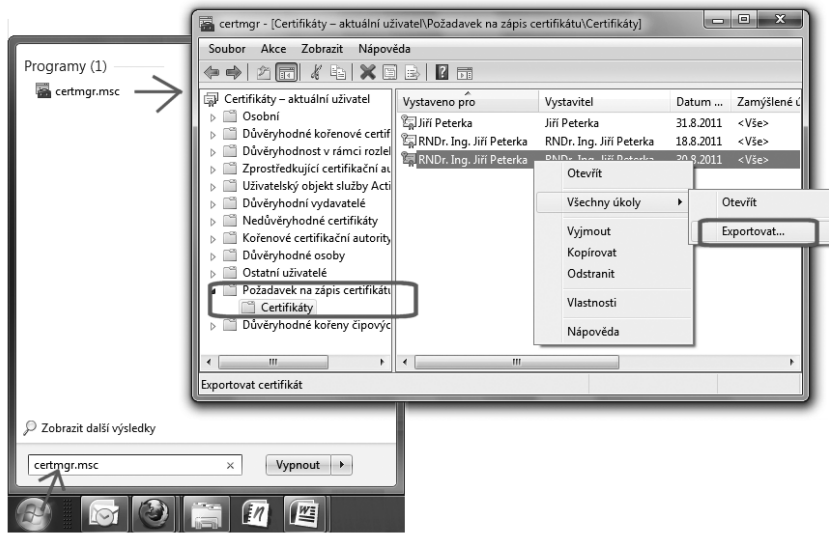
> V případě, kdy je exportován pouze samotný certifikát, bez soukromého klíče, jsou pro výstup nabízeny formáty PKCS#7, DER a PEM (poslední dva s příponou souboru .cer).

Právě popisovaného průvodce importem i exportem certifikátu z/do systémového úložiště certifikátů v MS Windows lze aktivovat více různými způsoby. Například přes volbu „instalovat certifikát“, kdykoli si jej prohlížíte prostřednictvím systémových prostředků MS Windows. Nebo při prohlížení obsahu systémového úložiště, například přes prohlížeč Internet Explorer (nabídka Nástroje, Možnosti Internetu, Obsah a pak Certifikáty).

Obrázek 5-67
Formáty pro export certifikátu bez soukromého klíče

V případě systémového úložiště MS Windows ale existuje jedna specifická situace, kdy se k obsahu tohoto úložiště nelze dostat „běžnými“ uživatelskými prostředky. Jde konkrétně o soukromý klíč, vygenerovaný v rámci žádosti o nový (či následný) certifikát právě do tohoto úložiště. Pokud jej uživatel potřebuje zazálohovat, pak pro přístup k němu musí využít speciální konzoli pro správu certifikátů: utilitu Certificate Manager (certmgr). Tu lze vyvolat napsáním jejího jména a přípony (certmgr.msc) do řádku pro spuštění, a pak potvrdit.

Obrázek 5-68
Utilita certmgr pro správu certifikátů v systémovém úložišti MS Windows



Utilita certmgr nabídne i ty složky systémového úložiště MS Windows, které jinak nejsou viditelné. Mezi nimi i složku „Požadavek na zápis certifikátu“, kam se ukládají soukromé klíče, vygenerované v rámci žádosti o vystavení certifikátu. A tyto klíče (i s dočasnými certifikáty s vlastním podpisem) pak lze pomocí této utility exportovat, viz obrázek (volba menu přes pravé tlačítko).

5.5.5 Revokace certifikátu

Do problematiky správy vlastních certifikátů patří i možnost jejich revokace, neboli možnost jejich předčasného zneplatnění (odvolání). Jak již víme z předchozích částí, je takováto možnost dostupná pouze v době řádné platnosti certifikátu.

Pokud bychom se podrobně začetli do certifikačních politik kvalifikovaných certifikačních autorit, zjistili bychom, že možnost revokovat náš vlastní certifikát má i sama certifikační autorita, a dokonce i dozorový orgán (Ministerstvo vnitra). To jsou ale možnosti, vycházející přímo z požadavků zákona a určené pro řešení opravdu výjimečných situací.[24]

Jiné opatření se týká zaměstnaneckých certifikátů a dává možnost pověřené osobě (zastupující zaměstnavatele) žádat nejen o vydání certifikátů pro konkrétní zaměstnance, ale i o jejich případnou revokaci. My si zde ale ukážeme, jak může požádat o revokaci vlastního certifikátu přímo jeho držitel.

Obecně lze konstatovat, že konkrétní postupy, kterými si lze revokaci vyžádat, stanovuje vydavatel certifikátu (certifikační autorita). V praxi jich bývá více a jsou odstupňovány podle toho, jak spolehlivě dokáže certifikační autorita identifikovat toho, kdo o revokaci žádá. Pokud jej dokáže identifikovat „na dálku“, může akceptovat i žádost zaslanou elektronickou cestou (mailem, přes web atd.). V opačném případě vyžaduje osobní návštěvu na pobočce a předložení osobních dokladů.

Pro identifikaci žadatele na dálku je nejčastěji využíváno speciální heslo (heslo pro zneplatnění). Toto heslo si uživatel obvykle určuje sám, a to již v rámci žádosti o vydání certifikátu, a bývá uvedeno v protokolu o vydání certifikátu. Později se jím musí prokázat, chce-li požádat o revokaci. Pokud si jej pamatuje, může revokaci provést například pomocí emailu či přes webové stránky certifikační autority, případně telefonicky.

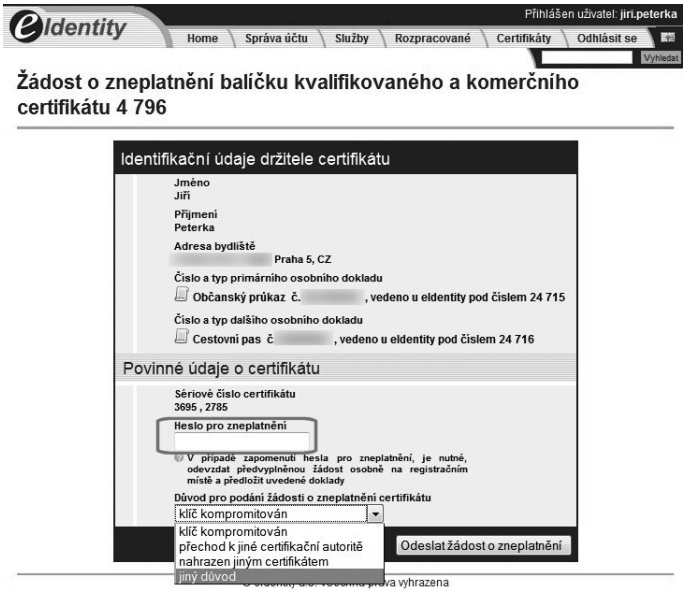
Příklad ukazuje následující obrázek, na kterém je žádost o zneplatnění certifikátu skrze webové stránky (u společnosti eIdentity, po úspěšném přihlášení do jejich klientského systému).

Kromě (povinného) hesla pro zneplatnění je zde možné uvést i důvod žádosti o zneplatnění certifikátu: zda došlo k jeho kompromitaci, či zda byl nahrazen jiným certifikátem apod.

---

[24] Sama certifikační autorita zneplatní certifikát v případě úmrtí držitele či jeho zbavení právní způsobilosti, ministerstvo zase může zneplatnit vydané certifikáty v případě odnětí akreditace certifikační autoritě apod.

Obrázek 5-69
Žádost o revokaci certifikátu přes webové stránky, u CA eIdentity



Konkrétní možnosti, jak požádat o revokaci certifikátu, se navíc mohou v čase měnit. Například CA PostSignum dříve umožňovala požádat o revokaci i skrze webové stránky, jen na základě zadání hesla pro zneplatnění (a bez jakéhokoli předchozího přihlašování).

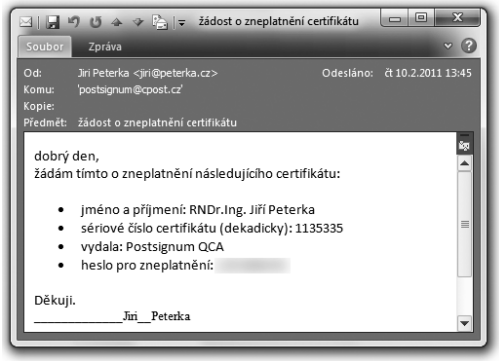
Možná ale, že tato varianta byla shledána málo bezpečná – a tak ji PostSignum již nepodporuje. Držitelé certifikátů od této certifikační autority (případně „pověřené osoby“) mohou dnes svou žádost doručit pouze osobně, telefonicky nebo e-mailem. Bez znalosti hesla pro zneplatnění ale stejně připadá v úvahu jen osobní návštěva.

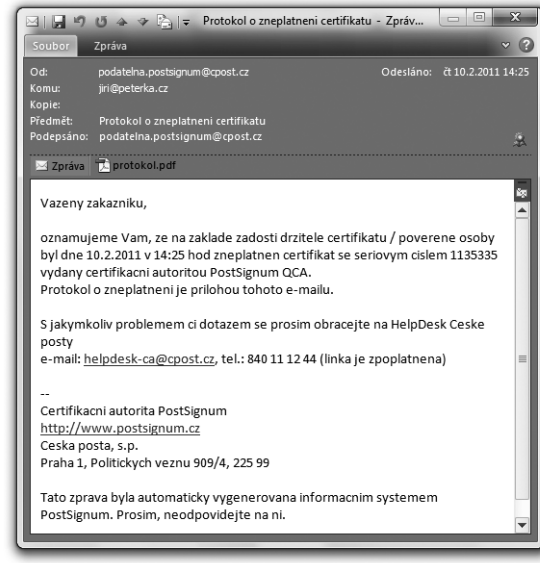
Ukažme si nyní příklad emailové žádosti o revokaci vlastního certifikátu, se znalostí hesla pro zneplatnění. Samotná žádost nemusí být nějak specificky formátována. Musí ale obsahovat předepsané náležitosti, konkrétně sériové číslo certifikátu, a také požadované heslo pro zneplatnění.

Na obrázcích na následující stránce si povšimněte i určitého časového rozdílu mezi okamžikem odeslání žádosti a okamžikem jejího přijetí. Zde je tato doba cca 40 minut, ale v praxi může být i výrazněji delší (třeba několik hodin), i v závislosti na denní době.

Okamžikem, ke kterému dochází k revokaci, přitom obvykle není okamžik podání, resp. přijetí žádosti o zneplatnění (na předchozím příkladu: 10. 2. 2011, 13:45), ale okamžik zpracování žádosti (zde: 14:25). Konkrétně u CA PostSignum je tento časový odstup v příslušné certifikační politice stanoven na max. 12 hodin – a do tohoto časového intervalu je zahrnuto i zveřejnění nového CRL seznamu.

Obrázek 5-70
Příklad e-mailové žádosti o zneplatnění certifikátu u CA PostSignum





Obrázek 5-71
Nově vydaný CRL seznam, již s informací o revokaci certifikátu (rozdíl jedné hodiny je dán jiným časovým pásmem)

6. PDF dokumenty a elektronický podpis

Kapitola 6

6. PDF dokumenty a elektronický podpis

V této kapitole se již dostaneme k tomu, jak se elektronický podpis používá v praxi. A to konkrétně u elektronických dokumentů, které jsou uloženy v souborech formátu **PDF** (**Portable Document Format**, dále jen **PDF dokumenty**). Takovéto dokumenty jsou v dnešní době hojně používané a při kontaktu s orgány veřejné moci často dokonce i vyžadované.

Ukážeme si, jak jednoduché a rychlé může být vytváření elektronických podpisů na PDF dokumentech, včetně připojování časových razítek, jakmile je vše zprovozněno a nastaveno, a hlavně funguje tak, jak má. Stejně tak si ukážeme, jak ověřovat platnost elektronických podpisů, elektronických značek a časových razítek na PDF dokumentech – a i zde uvidíme, že vše může být velmi jednoduché a současně také velmi spolehlivé. Opět ale jen za podmínky, že máme vše správně nastaveno a naše programy ověřují platnost podle správných pravidel a kritérií. Což zahrnuje i správně nastavený obsah právě používaného úložiště důvěryhodných certifikátů.

Než si ale ukážeme, jak PDF dokumenty podepisovat a opatřovat časovými razítky a jak vše ověřovat, měli bychom se nejprve seznámit s některými základními vlastnostmi tohoto formátu, které se vztahují právě k elektronickému podpisu.

Obecně můžeme konstatovat, že úplně všechny formáty dokumentů mohou být opatřovány externími podpisy a externími časovými razítky (viz část 2.8). Tím pádem lze externí elektronické podpisy používat i v souvislosti s dokumenty ve formátu PDF.

Pro interní elektronické podpisy ale takovéto konstatování již neplatí: zde již je nutná určitá podpora od příslušného formátu tak, aby „do něj“ bylo možné vkládat to, co tvoří elektronický podpis, značku či časové razítko. Takže interní elektronické podpisy podporují jen některé formáty dokumentů. Formát PDF mezi ně naštěstí patří.

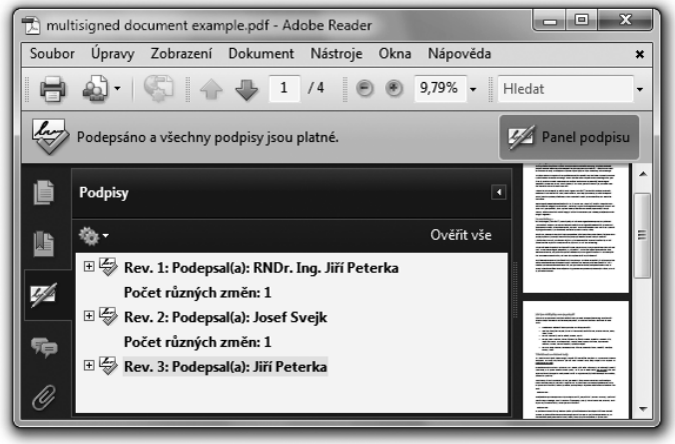
6.1 Interní podpisy PDF dokumentů

Formát PDF nabízí řadu možností pro interní elektronické podpisy, elektronické značky a časová razítka. Umožňuje například opatřit jeden a tentýž dokument více (interními) elektronickými podpisy.

Interní podpisy na PDF dokumentu přitom mohou být tzv. viditelné, či naopak neviditelné.[1]

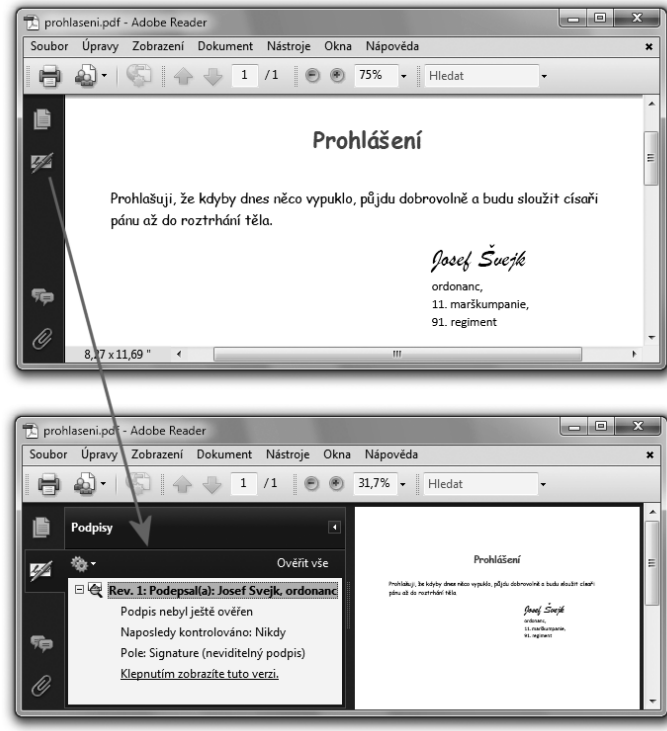
[1] Vedle těchto dvou základních variant ale PDF formát podporuje i dvě další varianty podpisů: **viditelný, ale netisknutý podpis** (který je zobrazován v těle dokumentu, ale není zahrnut do tisku), a dále **neviditelný, ale tisknutý podpis** (který není zobrazován v těle dokumentu, ale je naopak tisknut).

Obrázek 6-1
Příklad PDF dokumentu s více podpisy



Neviditelným elektronickým podpisem je míněno to, když na samotném elektronickém dokumentu – jak je uživateli zobrazován – není žádný elektronický podpis patrný a je „vidět“ pouze tehdy, pokud si jej uživatel nechá zobrazit prostředky toho prohlížeče, který právě používá.

Obrázek 6-2
Příklad neviditelného elektronického podpisu na PDF dokumentu

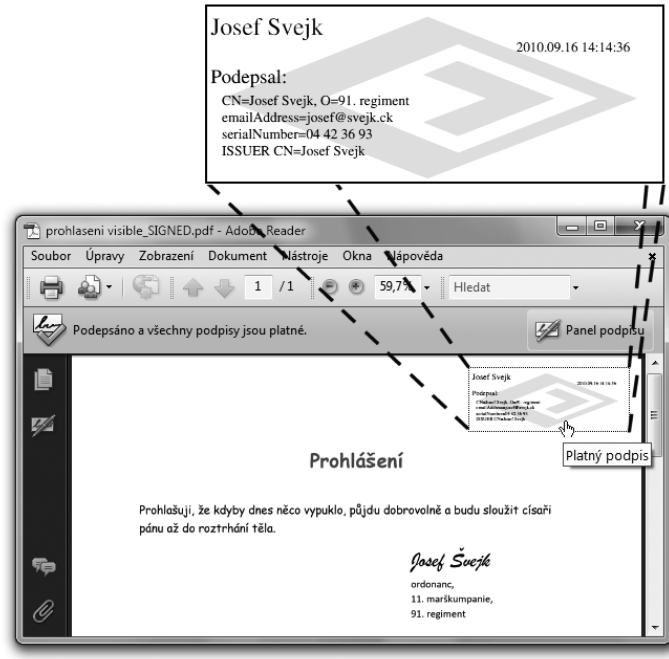


Stejné je to i při tisku PDF dokumentu (na papír): ani zde nebude patrné, že dokument je opatřen elektronickým podpisem. U papírového výtisku si navíc nemůžeme na nic kliknout a nechat si neviditelný podpis ukázat v samostatném okénku.

Možná i kvůli této nevýhodě se u PDF dokumentů zavedly také tzv. viditelné podpisy, které již jsou určitým způsobem patrné (viditelné) na samotném dokumentu tak, jak je tento uživateli zobrazován, i jak je tištěn.

Viditelný podpis má podobu podkladového obrázku, přes který je uveden text s údaji podepsané osobě, době podpisu, a případně i další údaje. Celý viditelný podpis pak je „vlepen“ do samotného dokumentu na místo, které určí uživatel – například v záhlaví první stránky, nebo na poslední stránce apod. Příklad ukazuje následující obrázek:

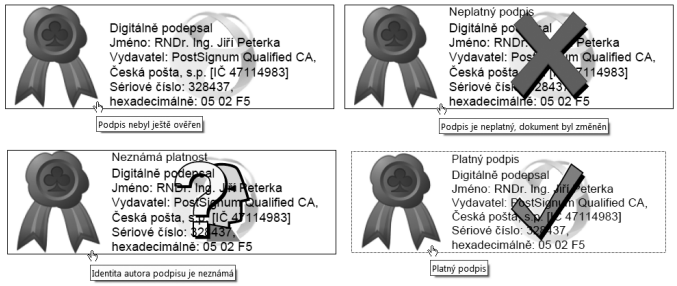
Obrázek 6-3
Příklad viditelného podpisu na PDF dokumentu



Může to tedy dopadnout například jako na dalším obrázku: po úspěšném ověření (platného) podpisu se obrázek na pozadí změní na zelenou fajfku, a při neplatnosti podpisu na červený křížek. Pokud verdikt zní „nevím“, obrázek se změní na žlutý otazník.

Obrázek 6-4

Příklad animovaného viditelného podpisu Takovéto „viditelné“ podpisy jsou někdy i animované, v tom smyslu že obrázková část takovéhoto viditelného podpisu se může měnit v závislosti na tom, zda a jak byl podpis vyhodnocen.

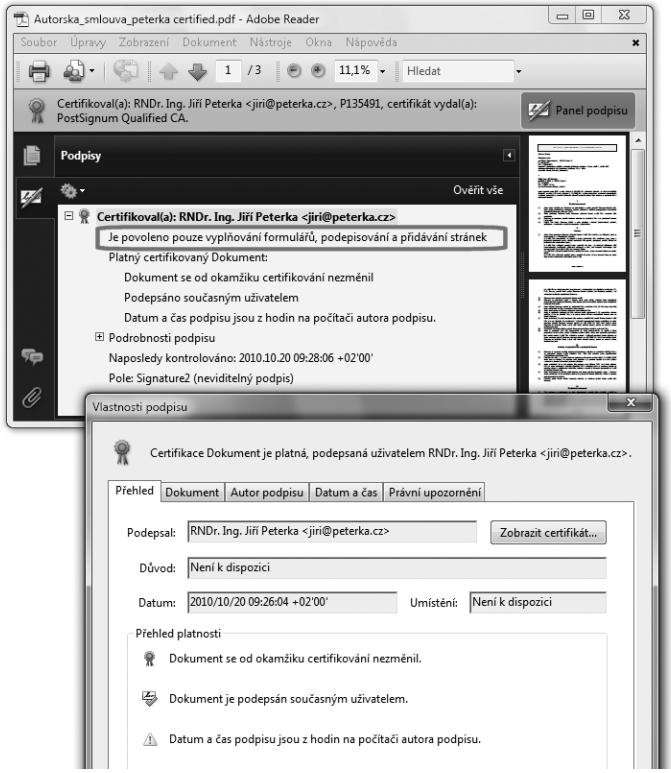


6.2 Certifikace PDF dokumentů

Formát PDF kromě podepisování podporuje ještě tzv. **certifikaci**. Ta se liší v tom, že připouští určité – rozsahem přesně vymezené – změny dokumentu i po jeho certifikaci.

Obrázek 6-5

Příklad certifikovaného dokumentu



Certifikace je řešením zejména pro formuláře ve formátu PDF, které někdo připraví, ale vyplňuje je již někdo jiný. A ten chce mít jistotu, že formulář je autentický: že nebyl pozměněn a že pochází skutečně od toho, kdo se vydává za jeho autora.

Pokud by ale byl takovýto formulář podepsán, neboli opatřen „běžným" elektronickým podpisem, byl by vlastně uzamknut vůči jakýmkoli změnám a nebylo by možné jej vyplňovat (protože jakákoli změna by porušila integritu podepsaného dokumentu.

Řešením je právě certifikace, resp. připojení certifikačního podpisu: jeho autor („certifikující osoba") sám určí, které části dokumentu (položky formuláře) mohou být změněny (vyplněny), aniž by došlo k porušení platnosti certifikace. A pokud by došlo ke změně nějaké jiné položky, certifikace by se stala neplatnou (stejně jako se při porušení integrity stává neplatným elektronický podpis).

Certifikace může být aplikována pouze na dosud nepodepsaný PDF dokument. Certifikační podpis proto musí být prvním podpisem na PDF dokumentu ve smyslu pořadí jejich přidávání. Následně pak může (ale samozřejmě nemusí) být PDF dokument opatřen jedním či několika „klasickými" elektronickými podpisy. Ty pak, v případě formuláře, stvrzují vyplněný obsah.

Certifikace může mít pouze interní charakter (ve smyslu rozdílu mezi interním a externím elektronickým podpisem), ale může být jak viditelná, tak i neviditelná. Příklad toho, jak je certifikace zobrazována programem Adobe Reader, ukazuje obrázek na předchozí stránce.

Zajímavou otázkou kolem certifikačních podpisů je jejich právní statut: lze je považovat za zaručené elektronické podpisy, a v závislosti na certifikátu i za uznávané podpisy? Odpověď, vyplývající ze sdělení MV ČR, je taková že certifikační podpis je možné považovat za zaručený elektronický podpis, pokud u něj nedošlo k žádné změně od vzniku certifikačního podpisu.[2]

Certifikační podpisy lze vytvářet pouze programem Adobe Acrobat,[3] nikoli programem Adobe Reader. Proto si konkrétní postup vytváření těchto podpisů ukážeme až při popisu možností podepisování právě pomocí programu Adobe Acrobat.

---

[2] Jde o vyjádření Odboru koncepce a koordinace ICT ve veřejné správě MVČR na dotaz autora této knihy, ze dne 23.11.2010: „*z pohledu zákona o elektronickém podpisu je podepsán pouze ten dokument, ve kterém k žádné (ani autorem povolené) změně nedošlo, neboť pouze s tímto dokumentem je podpis logicky svázán, jak vyžaduje §2 odst. a) zákona o elektronickém podpisu. Certifikovaný dokument bez provedených změn JE tedy opatřen zaručeným elektronickým podpisem*".

[3] Ale stejně tak lze vytvářet certifikační podpisy i některými programy třetích stran, nikoli od společnosti Adobe.

6.3 Časová razítka na PDF dokumentech

Časová razítka jsou u PDF dokumentů pojímána poněkud odlišně od představy, kterou jsme si až doposud budovali: že razítko je „něco samostatného“, co se aplikuje nezávisle na elektronických podpisech (typicky někdy „po podpisu“, aby fixovalo jeho existenci v čase), je založeno na svém vlastním certifikátu, také se samostatně ověřuje a má „svou vlastní“ platnost. A že také z pohledu práva má svůj vlastní a specifický statut.

U PDF dokumentů je ale časové razítko standardně vnímáno jako něco nesamostatného. Jako atribut časového údaje, který je součástí elektronického podpisu.

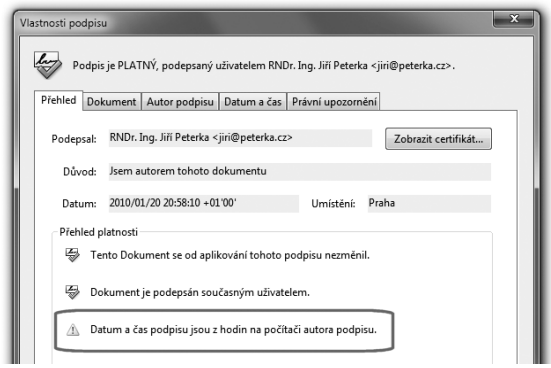
Jinými slovy: bez časového razítka se do elektronického podpisu vkládá časový údaj, převzatý ze systémových hodin počítače. A jelikož tyto systémové hodiny si uživatel může libovolně posunout, nelze se na tento údaj spoléhat. V opačném případě se do elektronického podpisu vloží údaj o čase, pocházející z časového razítka. A tedy garantovaný časový údaj, na který se již lze spolehnout.[4]

> Lze si to představit také tak, že časové razítko je zde jakoby vloženo přímo do samotného elektronického podpisu.

Praktický důsledek je ten, že PDF dokument nelze (až na výjimku, viz dále) opatřit samostatným časovým razítkem. Místo samostatného časového razítka je možné k PDF dokumentu přidat pouze další elektronický podpis, obsahující vložené časové razítko (podpis, jehož časový údaj je převzat z časového razítka).

Indikaci rozdílu v „kvalitě“ časových údajů, obsažených v elektronických podpisech na PDF dokumentech, ilustrují následující obrázky. Na prvním z nich je dokument, jehož elektronický podpis obsahuje údaj o čase, převzatý ze systémových hodin místního počítače (zvýrazněno červeně).

Obrázek 6-6
Podpis bez časového razítka (časový údaj je převzat z hodin počítače)

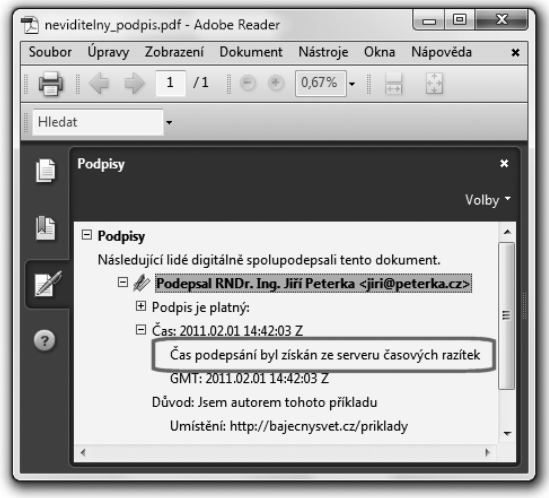


[4] Samozřejmě jen pokud jde o časový údaj o kvalifikovaného poskytovatele časových razítek.

Tato skutečnost je zdůrazněna i volbou ikony (žlutý trojúhelník s vykřičníkem, naznačující potenciální nespolehlivost údaje).

Na dalších obrázcích pak jsou elektronické podpisy, které již obsahují časové razítko, resp. časový údaj, převzatý z časového razítka. První z nich ukazuje, jak tuto skutečnost signalizuje Adobe Reader verze 8. x: používá výstižnou formulaci „*Čas podepsání byl získán ze serveru časových razítek*“.

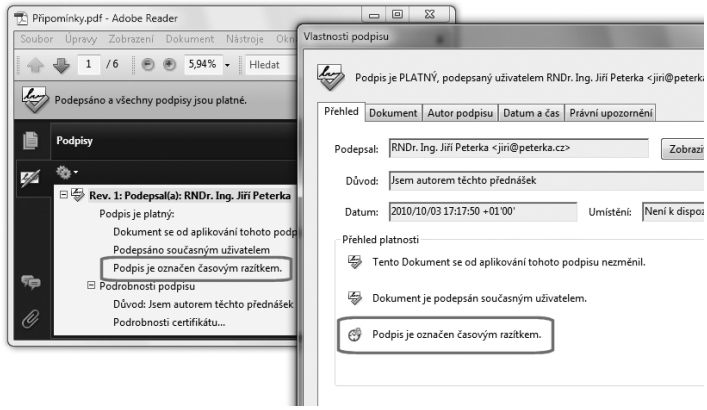
Obrázek 6-7
Podpis, obsahující časové razítko (Adobe Reader 8.x)



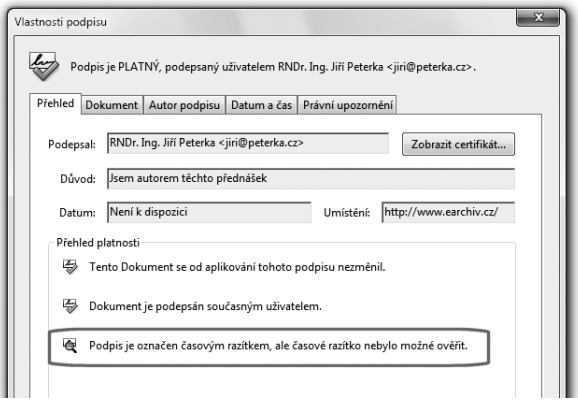
Z hlediska „manipulace“ je tedy časové razítko na PDF dokumentech nesamostatné – nelze jej přidat samostatně (nezávisle na elektronickém podpisu), ani jej samostatně odebrat. Proto je někdy označováno také jako **„podpisové“ časové razítko** (anglicky **signature timestamp**).

Z hlediska své platnosti je i takovéto „podpisové“ časové razítko přeci jen samostatné: v tom smyslu, že je založeno na samostatném (systémovém) certifikátu, a proces jeho ověřování (vyhodnocování platnosti) probíhá samostatně a nezávisle na ověřování samotného podpisu.

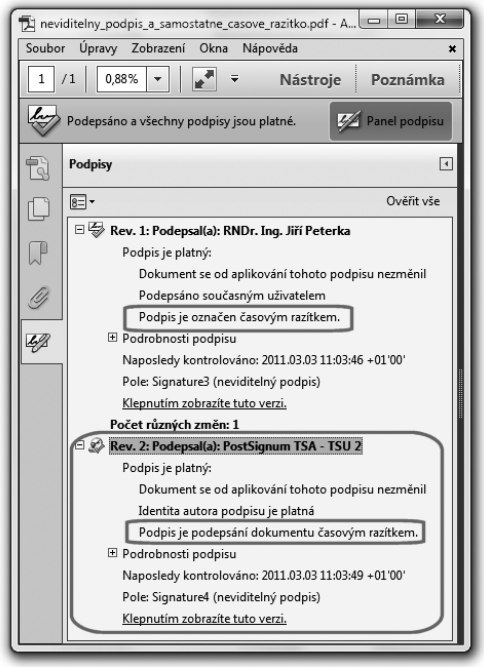
Může se tedy stát například to, že časové razítko bude vyhodnoceno jako platné, zatímco podpis nikoli (ověření podpisu skončí verdiktem „nevíme“).



Obrázek 6-8
Podpis, obsahující časové razítko (Adobe Reader 9.x)



Obrázek 6-9
Příklad platného podpisu s časovým razítkem, jehož ověření se nepodařilo.



Obrázek 6-10
Příklad PDF dokumentu s elektronickým podpisem (vč. „podpisového“ časového razítka) a se samostatným „archivním“ časovým razítkem, v programu Adobe Reader verze X

Nebo podpis může být platný, zatímco u časového razítka skončí vyhodnocení verdiktem „nevím“. Příklad ukazuje prostřední obrázek na protilehlé straně.

Samozřejmě připadají v úvahu i všechny další kombinace. Může být platný jak podpis, tak i časové razítko. Nebo mohou být oba neplatné atd.

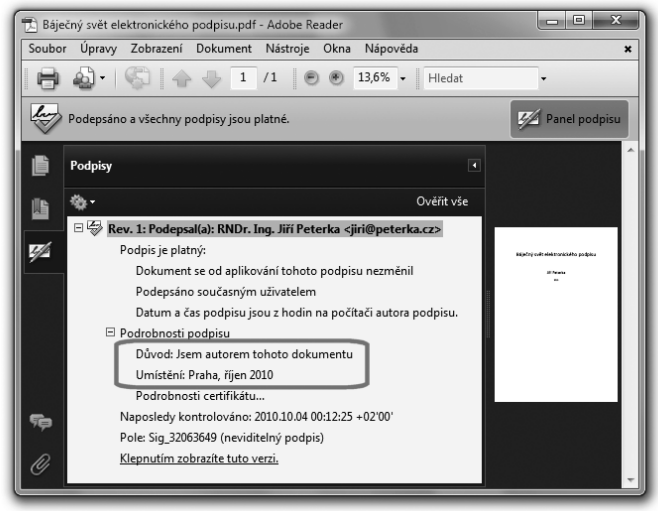
Avizovanou výjimkou z principu, že k PDF dokumentům nelze přidávat samostatná časová razítka, je podpora „archivních“ časových razítek (v rámci podpory konceptu PAdES) u produktů Adobe verze X. Tedy u programů Adobe Acrobat X a Adobe Reader X. Ty již dokáží připojovat k PDF dokumentu samostatná časová razítka – ale bez zpětné kompatibility, takže starší verze Readeru a Acrobatu je nedokáží ověřit.

Podrobněji si problematiku archivních časových razítek popíšeme v části 6.11.

6.4 Důvod a místo podpisu

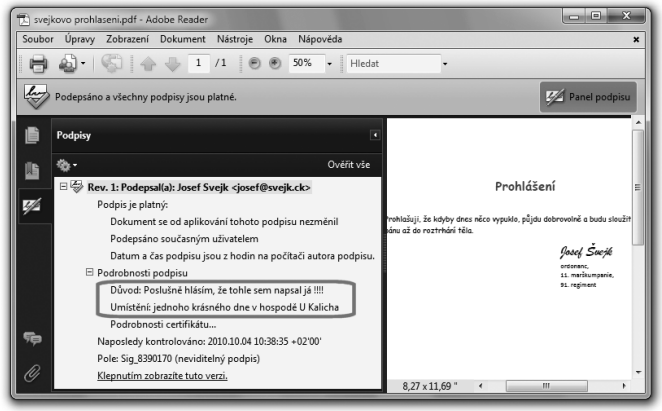
S elektronickými podpisy na PDF dokumentech mohou být spojeny i některé další informace. Například důvod podpisu či místo, kde k podpisu došlo (ve smyslu geografické lokality). Případně i kontaktní údaje na podepsanou osobu apod. Příklad ukazuje obrázek.

Obrázek 6-11
Příklad důvodu a místa podpisu



Zdůrazněme si ale, že jde skutečně jen o informace, které je třeba brát jako zcela nezávazné. Ten, kdo podpis vytváří, si je totiž mohl nastavit (vyplnit) zcela podle své libosti. Takže mohou, ale také vůbec nemusí, korespondovat se skutečností, resp. být pravdivé.

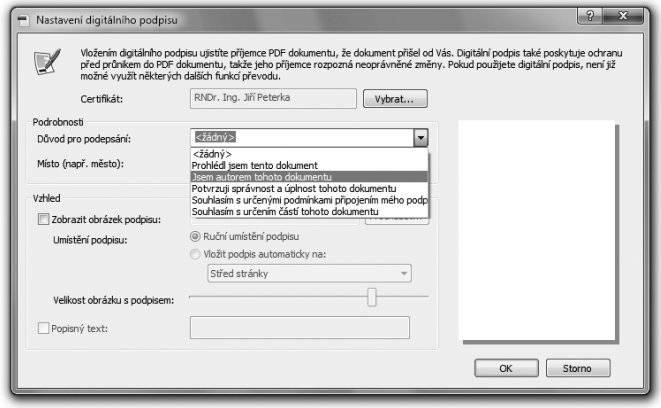
Obrázek 6-12
Ukázka možnosti libovolně vyplnit důvod i umístění



Důležité je také to, že tyto informace nemají oporu v platné legislativě, týkající s elektronického podpisu – ten takovéto „dodatečné informace“ vůbec nezná. I proto se na ně nemůžeme spoléhat. Určitě ne takovým způsobem, jakým se spoléháme na údaje, obsažené například v kvalifikovaném certifikátu.

Na druhou stranu i takovéto (zcela nezávazné) informace mohou mít svůj význam a smysl. Mohou nám pomoci hlavně při hodnocení toho, proč někdo připojil k dokumentu svůj elektronický podpis. Na to ostatně pamatují i obvyklé „předdefinované“ důvody, připravené v nástrojích pro vytváření elektronických podpisů, viz následující obrázek.

Obrázek 6-13
Příklad nabídky předdefinovaných důvodů podpisu (u programu Print2PDF od Software602)



Znovu si ale zdůrazněme, že na žádné „důvody podpisu“ není v zákonné úpravě elektronického podpisu pamatováno.

6.5 Ověřování interních elektronických podpisů v programu Adobe Reader

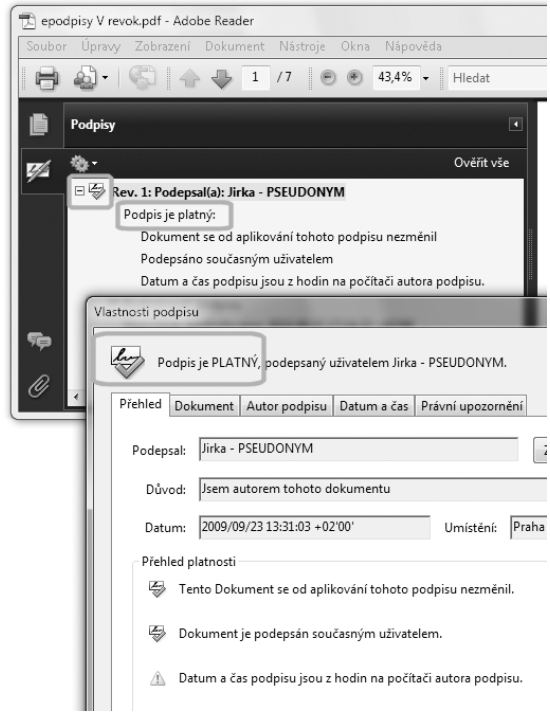
Ověřování elektronických podpisů pomocí volně šiřitelného programu Adobe Reader je na první pohled velmi jednoduché, až triviální – a jeho verdikty v prvním přiblížení velmi dobře korespondují s tím, co jsme si o ověřování platnosti podpisů říkali již ve 3. kapitole.

Připomeňme si, že výsledek ověření platnosti elektronického podpisu může mít tři různé výsledky:

- „ano“, resp. podpis je platný
- „ne“, resp. podpis je neplatný
- „nevím“, resp. nejsme schopni ověřit planost podpisu.

Třemi různými výsledky může skončit i ověření elektronického podpisu, které provádí program Adobe Reader. Ukažme si je postupně na obrázcích, ze kterých bude patrné, jak je výsledek rozlišen textově i graficky.

První možností je, když Adobe Reader konstatuje: „podpis je platný“. To jednak napíše, a ještě to zdůrazní zeleným symbolem „fajfky“, viz obrázek.

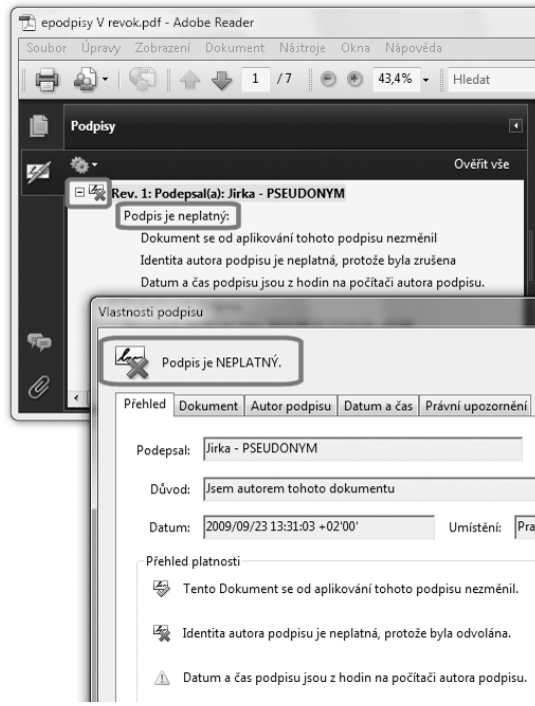


Obrázek 6-14
Adobe Reader konstatuje, že podpis je platný

Druhou možností je, když Adobe Reader konstatuje: „podpis je neplatný“. To zdůrazní červeným symbolem křížku, a samozřejmě také napíše slovně, viz obrázek na této stránce. Konečně třetí možností je, když Adobe Reader konstatuje, že platnost podpisu je neznámá. To znázorní žlutým symbolem trojúhelníku s vykřičníkem, viz obrázek na další stránce.

Mějme ale vždy na paměti jednu nesmírně důležitou skutečnost: tři různé verdikty programu Adobe Reader vůbec nemusí korespondovat se třemi možnými výsledky ověření elektronického podpisu ve smyslu zákona (resp. tak, jak jsme si toto ověřování popisovali v kapitole 3).

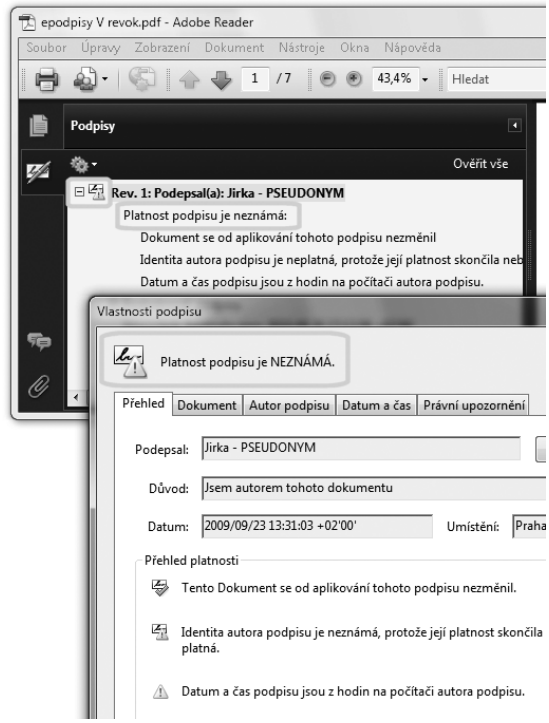
Obrázek 6-15
Adobe Reader konstatuje, že podpis je neplatný



Mementem budiž to, čeho si pozorný čtenář může povšimnout na třech posledních obrázcích (na předchozí, této a následující stránce): všechny tři ukazují výsledek ověření jednoho a téhož elektronického podpisu (na stejném dokumentu). Podpis na něm vyhodnotil Adobe Reader poprvé jako platný, podruhé jako neplatný a potřetí konstatoval, že jeho platnost nedokáže posoudit (že je pro něj neznámá).

Uvedené tři obrázky přitom nejsou nijak zretušované či jinak „podvržené“. Právě naopak, věrně ukazují různé (a věcně správné) chování programu Adobe Reader v závislosti na tom, jak je právě nastaven.

Pamatujme si tedy, že pravidla, podle kterých Adobe Reader ověřuje elektronické podpisy, jsou významně ovlivněna jeho nastavením. Do té míry, že jeho výsledné hodnocení může být zcela odlišné pro různá nastavení.



Obrázek 6-16
Adobe Reader konstatuje, že platnost podpisu je neznámá

První obrázek (obrázek 6-14) ukazuje verdikt Adobe Readeru v situaci, kdy mu bylo zakázáno kontrolovat stav revokace certifikátu a současně mu bylo řečeno, že posuzovaným okamžikem (tj. okamžikem, ke kterému má podpis ověřovat) má být okamžik údajného vzniku podpisu (tj. časový okamžik, který je uveden přímo v samotném podpisu). Za těchto podmínek Reader (správně) vyhodnotil podpis jako platný.

Druhý obrázek (obrázek 6-15) ukazuje verdikt v situaci, kdy je kontrola revokace povolena (a je zjištěno, že certifikát byl revokován), a současně je Adobe Reader nastaven tak, aby posuzovaným okamžikem byl aktuální okamžik. Za těchto podmínek Adobe Reader správně vyhodnotil podpis jako neplatný (protože k aktuálnímu okamžiku byl certifikát již revokovaný).

Třetí obrázek (obrázek 6-16) naopak ukazuje verdikt v situaci, kdy kontrola revokace byla opět zakázána, a posuzovaným okamžikem byl aktuální časový okamžik. Zde Adobe Reader konstatoval, že platnost podpisu je neznámá, protože k posuzovanému okamžiku již skončila řádná platnost certifikátu, na kterém je podpis založen.

Správné nastavení Adobe Readeru tak, aby postupoval podle pravidel popsaných v kapitole 3, by odpovídalo druhému z výše uvedených případů: jelikož dokument neobsahuje časové razítko (resp. podpis obsahuje časový údaj převzatý ze systémových hodin a nikoli z časového razítka), nemůžeme se na oka-

mžik vzniku spoléhat a musíme platnost podpisu ověřovat k aktuálnímu okamžiku. Samozřejmě musíme kontrolovat revokaci certifikátu – a jelikož k revokaci došlo před aktuálním okamžikem, musíme podpis považovat za neplatný (protože nedokážeme rozhodnout, zda vznikl ještě před revokací, nebo až po ní).

Zdůrazněme si proto znovu, že má-li mít verdikt programu Adobe Reader při ověřování elektronických podpisů vůbec smysl, musí být tento program správně nastaven.

Bohužel takovéto „správné nastavení“ (které by dávalo výsledky odpovídající platné právní úpravě elektronického podpisu v ČR), není shodné s implicitním nastavením programu Adobe Reader (které určuje jeho „standardní“ chování). Je tedy nutné jeho nastavení upravit tak, aby Adobe Reader ověřoval (interní) elektronické podpisy v souladu s platnou právní úpravou.

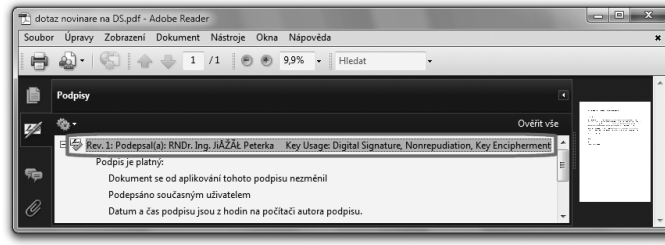
Celkově je nutné konstatovat, že Adobe Reader není bezpečným prostředkem pro ověřování elektronických podpisů tak, jak jej chápe zákon č. 227/2000 Sb. (o elektronickém podpisu). Není nijak certifikován ani jinak zkoumán z pohledu toho, jak dalece naplňuje požadavky tohoto zákona. Na druhou stranu naše legislativa používání bezpečných prostředků (pro vytváření i ověřování podpisů) nevyžaduje.

Reader proto musíme brát jako komerční program, který má určité chování (stanovené jeho výrobcem) a jako uživatelům nám poskytuje určité informace. A je na nás, abychom tyto informace správně interpretovali.

6.5.1 Identita podepsané osoby

To, že Adobe Reader nemůžeme považovat za bezpečný prostředek pro ověřování elektronických podpisů ve smyslu zákona, lze dokumentovat nejen na tom, jak moc je jeho chování a hodnocení závislé na různých nastaveních. Dalším důvodem může být i způsob, jakým poskytuje informace o identitě podepsané osoby.

Příklad vidíme na následujícím obrázku, který naznačuje, že do řetězce popisujícího identitu podepsané osoby se mohou dostat i různé „nestandardní“ znaky a dokonce i části textu, očividně pocházející odjinud, než by měly (z jiných položek certifikátu).

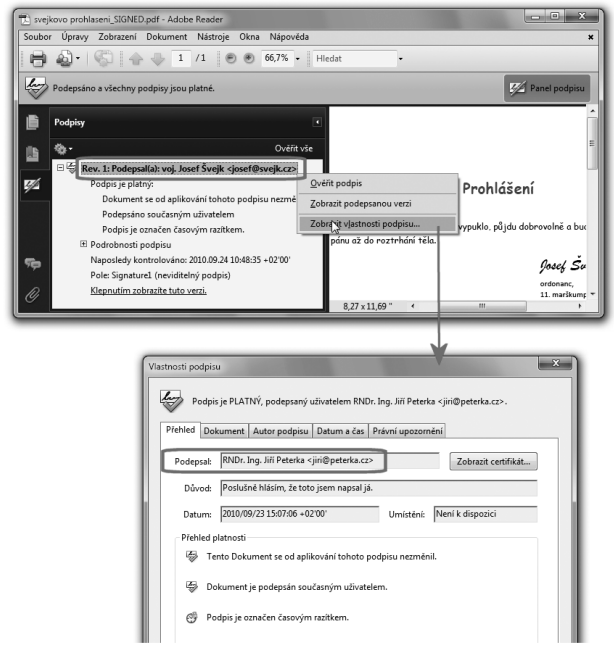


Obrázek 6-17
Příklad nestandardních znaků a jiného obsahu v údajích o podepsané osobě (tak jak zobrazuje Adobe Acrobat)

Ještě významnější je ale další příklad na následující stránce, který ukazuje, že na údaj o identitě podepsané osoby – tak, jak se zobrazuje u neviditelného podpisu (v panelu pro podpisy) v programu Adobe Reader – se vůbec nemůžeme spoléhat. V zásadě obsahuje jen textový řetězec, který je při vytváření podpisu možné nastavit zcela libovolně (zřejmě jako jakýsi alias). Zde byla do tohoto řetězce vložena identita literární postavy Josefa Švejka – a Adobe Reader ji zobrazuje tak, že může být snadno zaměněna za skutečnou identitu podepsané osoby.[5]

Obrázek 6-18

Příklad toho, kdy se liší údaje o podepsané osobě (tak, jak je zobrazuje Adobe Reader)



Dostupné údaje o identitě podepsané osoby tedy spolehlivě zjistíme až z obsahu certifikátu, na kterém je podpis založen.

To, zda Adobe Reader u interního podpisu zobrazuje údaje pocházející z certifikátu, nebo „libovolně nastavitelný“ řetězec (jako v právě uvedeném příkladu) navíc záleží na způsobu jeho ovládání. Pokud má Adobe Reader nastaveno automatické ověřování všech podpisů již při otevírání elektronického dokumentu, pak situace z obrázku nenastává (a v panelu podpisu se objeví stejný údaj o podepsané osobě, jaký je uveden na certifikátu). Pokud je ale automatické ověřování podpisů vypnuto a uživatel si ověření vyžádá „ručně“ (přes panel podpisu), pak je naopak zobrazen onen libovolně nastavitelný řetězec (zde s identitou Josefa Švejka). Jde zřejmě o chybu programu.[6]

5 PDF dokument s tímto příkladem si můžete stáhnout na *http://www.bajecnysvet.cz/priklady/neshoda.php*

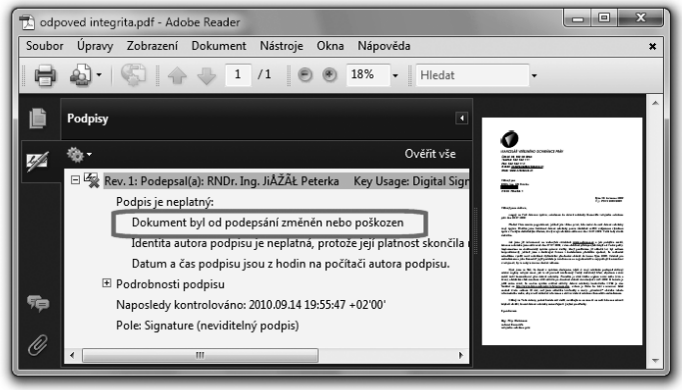
6 Která se vyskytuje u Adobe Readeru a Acrobatu ve verzích 8, 9 i X.

6.5.2 Kontrola integrity podepsaného dokumentu

Abychom si mohli popsat vliv dalších nastavení Adobe Readeru, musíme si nejprve přiblížit jeho konkrétní postup při ověřování elektronických podpisů (ale i značek a razítek). Abychom věděli, co a jak dělá a co naopak nedělá.

Posloupnost hlavních kroků odpovídá postupu, který jsme si popisovali v kapitole 3. To znamená, že nejprve Adobe Reader posoudí integritu podepsaného dokumentu. Pokud je porušena, ihned prohlásí celý podpis za neplatný. A v tomto se zcela shoduje se správným postupem „podle práva".

Obrázek 6-19
Neplatný elektronický podpis z důvodu porušení integrity



Takže pokud Adobe Reader skončí ověřování konstatováním, že podpis není platný z důvodu porušení integrity, můžeme mu věřit a jeho verdikt brát jako bernou minci, ať je jeho nastavení jakékoli. Zkoumání integrity je totiž zcela nezávislé na možnostech jeho nastavení.

Není-li integrita podepsaného dokumentu porušena, snaží se Adobe Reader zkoumat platnost toho certifikátu, na kterém je podpis založen. Aby tak ale mohl činit, musí nejprve rozhodnout, k jakému časovému okamžiku tak bude činit. Tedy zvolit to, co jsme si v kapitole 3 pojmenovali jako „posuzovaný okamžik".

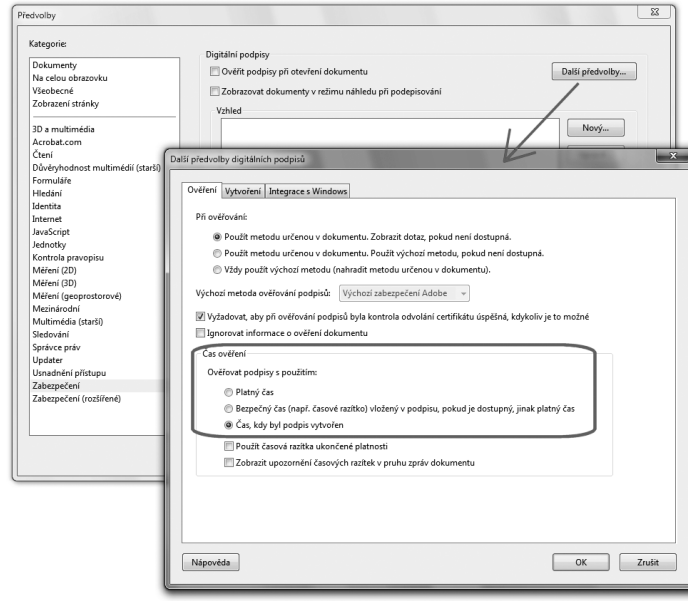
6.5.3 Volba posuzovaného okamžiku

Volba posuzovaného okamžiku je již jednou z věcí, které se programu Adobe Reader nastavují, a to na jednu z následujících tří možností:

- **platný čas**: posuzovaným okamžikem bude aktuální časový okamžik
- **bezpečný čas:** posuzovaným okamžikem bude čas, uvedený na (podpisovém) časovém razítk Přesněji čas, uvedený přímo v samotném podpisu, pokud pochází z časového razítka (viz výše). Nepochází-li údaj z časového razítka, bude posuzovaným časovým okamžikem aktuální časový okamžik (tj. tato druhá možnost přejde v první možnost)

- **čas, kdy byl podpis vytvořen:** posuzovaným okamžikem bude časový okamžik, uvedený přímo v podpisu jako okamžik jeho vzniku – bez ohledu na to, zda pochází z časového razítka nebo ze systémových hodin.

Na následujícím obrázku je vidět možnost volby těchto tří možností: v menu Readeru přes Úpravy, Předvolby, Zabezpečení, Další předvolby, Ověření a Čas ověření.



Obrázek 6-20
Nastavení posuzovaného okamžiku v Adobe Readeru

Důležité je, že implicitně (tj. bezprostředně po instalaci nového Adobe Readeru)[7] je nastavena třetí možnost, tedy „čas, kdy byl podpis vytvořen“. Což je logicky správná volba, protože posuzovat platnost podpisu bychom skutečně měli k okamžiku, kdy byl vytvořen. Naráží to ale na problém, diskutovaný již v části 2.6.2: že na tento časový okamžik, který je uveden přímo v samotném podpisu, se nemůžeme spoléhat. Přesněji nemůžeme se na něj spoléhat v případě, kdy tento časový údaj pochází ze systémových hodin počítače, na kterém podpis vznikl, a nikoli od nějakého (kvalifikovaného) poskytovatele služby časových razítek.

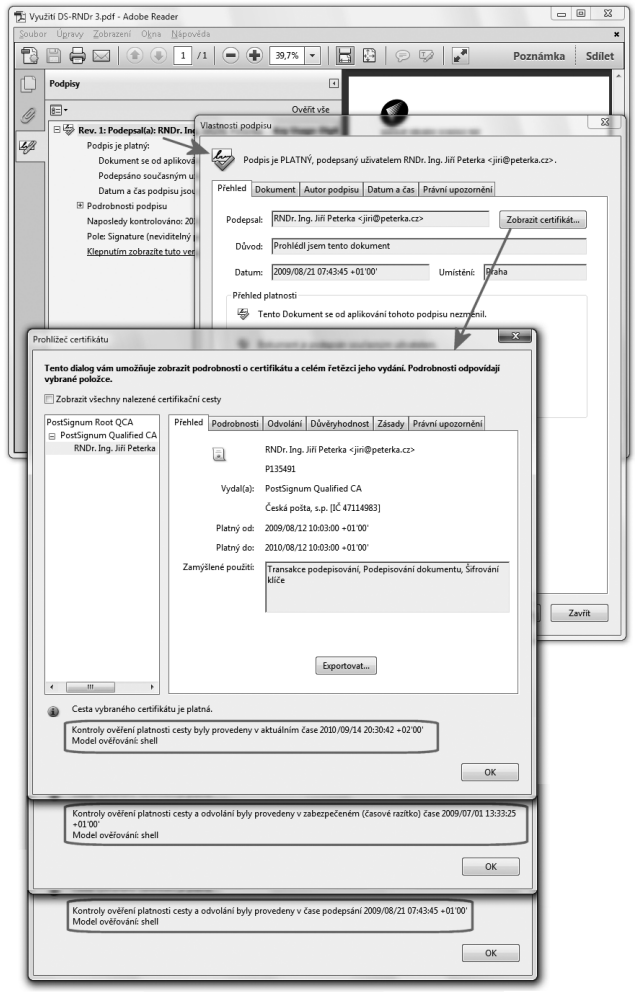
Správně bychom měli zvolit prostřední volbu, neboli „bezpečný čas“. Tedy buďto čas na časovém razítku, nebo čas aktuální.

To, jaký konkrétní čas byl při vyhodnocování platnosti (ověřování) konkrétního elektronického podpisu nakonec doopravdy použit, resp. brán v úvahu, si jako uživatelé můžeme zkontrolovat, díky tomu že Adobe Reader (a stejně tak Acrobat) tuto informaci zobrazuje.

[7] Toto platí od verze 9.1. U předchozích verzí byla implicitně nastavována možnost „Bezpečný čas“.

Příslušnou informaci najdeme v okně s detaily certifikátu, na kterém je podpis založen, viz následující obrázek. Ten ukazuje možný výsledek pro všechny tři varianty nastavení posuzovaného okamžiku.

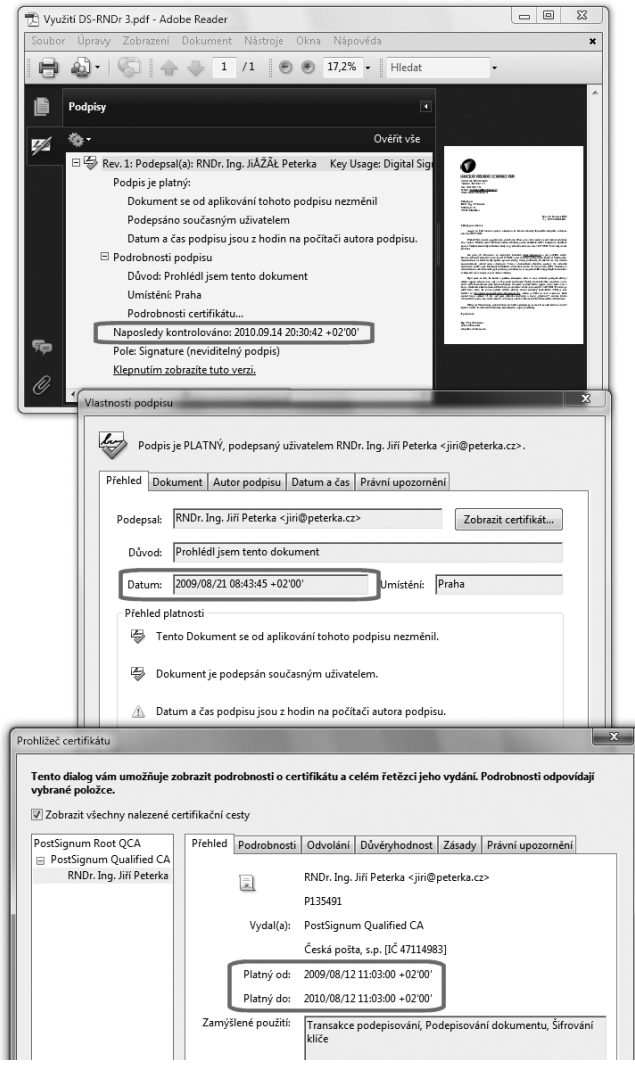
Obrázek 6-21
Indikace skutečně použitého posuzovaného okamžiku



Stále ale mějme na paměti, že dopady nesprávného nastavení posuzovaného okamžiku jsou zcela zásadní, jak jsme si ostatně již naznačovali výše.

Ukažme si to podrobněji na následujícím příkladu PDF dokumentu, který měl být podepsán 21. 8. 2009, ale podpis není opatřen (podpisovým) časovým razítkem. Údaj o době vzniku tedy pochází od systémových hodin počítače, a tudíž se na něj nemůžeme spoléhat.

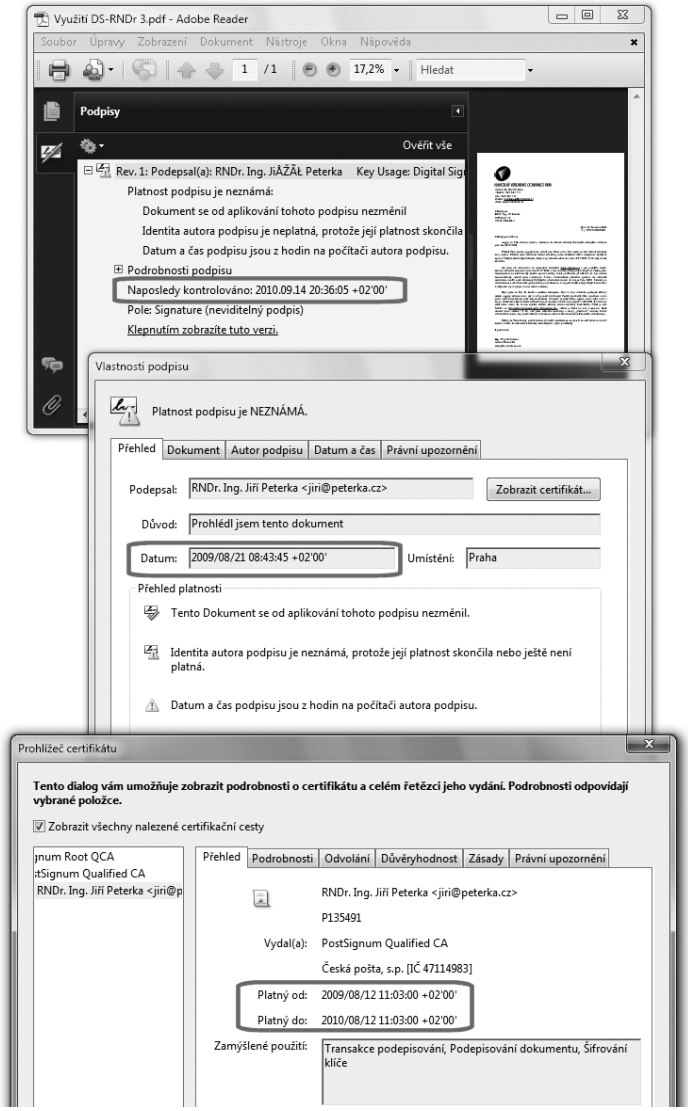
Obrázek 6-22
Podpis, vyhodnocený jako platný – když posuzovaný okamžik je okamžikem vzniku podpisu



Předpokládejme také, že podpis je založen na certifikátu, jehož řádná platnost trvala od 12. 8. 2009 do 12. 8. 2010, a v této řádné době své platnosti nebyl certifikát revokován. Předpokládejme dále, že platnost byla ověřována dne 14. 9. 2010.

Pokud bylo při ověřování platnosti ponecháno implicitní nastavení Readeru, byl podpis ověřen jako platný. Tak to ukazuje i obrázek na této stránce. Posuzovaným okamžikem totiž byl „čas, kdy byl podpis vytvořen“, zde tedy 21. 8. 2009 – a v té době byl příslušný certifikát ještě platný (a nerevokovaný).

Jelikož ale podepsaný PDF dokument nebyl opatřen (podpisovým) časovým razítkem, spoléhali jsme se zde na něco, o čem nemáme jistotu: že podpis skutečně vznikl 21. 8. 2009. Nemůžeme proto vyloučit, že podpis ve skutečnosti vnikl někdy později, na počítači s „přetočenými hodinami“. Mohl jej vytvořit například někdo, kdo se podvodně zmocnil příslušného soukromého klíče v době, kdy příslušný certifikát již expiroval a jeho majitel jej již nemohl revokovat (viz část 3.4.5).



Obrázek 6-23
Podpis s neznámou platností – při ověřování podle aktuálního času

Právě kvůli tomu, že bez časového razítka takovouto možnost nemůžeme vyloučit, musíme (v souladu s pravidly, formulovanými v kapitole 3) posuzovat platnost podpisu k aktuálnímu časovému okamžiku (zde: 14. 9. 2010).

Pak ale ověření podpisu nutně musí skončit výsledkem „nevím“, protože k uvedenému posuzovanému okamžiku již skončila platnost certifikátu a na jeho obsah se tak není možné spoléhat.

Ke stejnému závěru došel i Reader, pokud mu byl (správně) nastaven posuzovaný okamžik na prostřední variantu, neboli na „bezpečný čas“.

Na základě tohoto nastavení se Adobe Reader nejprve snažil použít čas, pocházející z časového razítka. To ale nebylo k dispozici, a tak Reader nakonec použil aktuální čas v době posuzování.

Posouzení stejného dokumentu jako na předchozím příkladu (podepsán 21. 8. 2010, certifikátem s platností do 12. 8. 2010, bez časového razítka, ověřováno 14. 9. 2010) pak již skončilo správným verdiktem: „nevím“, resp. „platnost podpisu je neznámá“, viz předchozí obrázek.

Pamatujme si dobře tento příklad: Adobe Readeru je třeba správně nastavit, co má považovat za posuzovaný okamžik. Pokud to neuděláme, může posuzovat platnost podpisu i podle negarantovaného údaje o čase, který si podpis nese přímo v sobě a který nepochází z časového razítka, nýbrž ze snadno zmanipulovatelných systémových hodin na počítači.

Správně bychom tedy měli Adobe Readeru nastavit posuzovaný okamžik na „bezpečný čas“, při kterém již je bráno v úvahu časové razítko a použit v něm uvedený čas, nebo je podpis ověřován k aktuálnímu času (není-li k dispozici časový údaj z razítka).

6.5.4 Kontrola revokace certifikátu

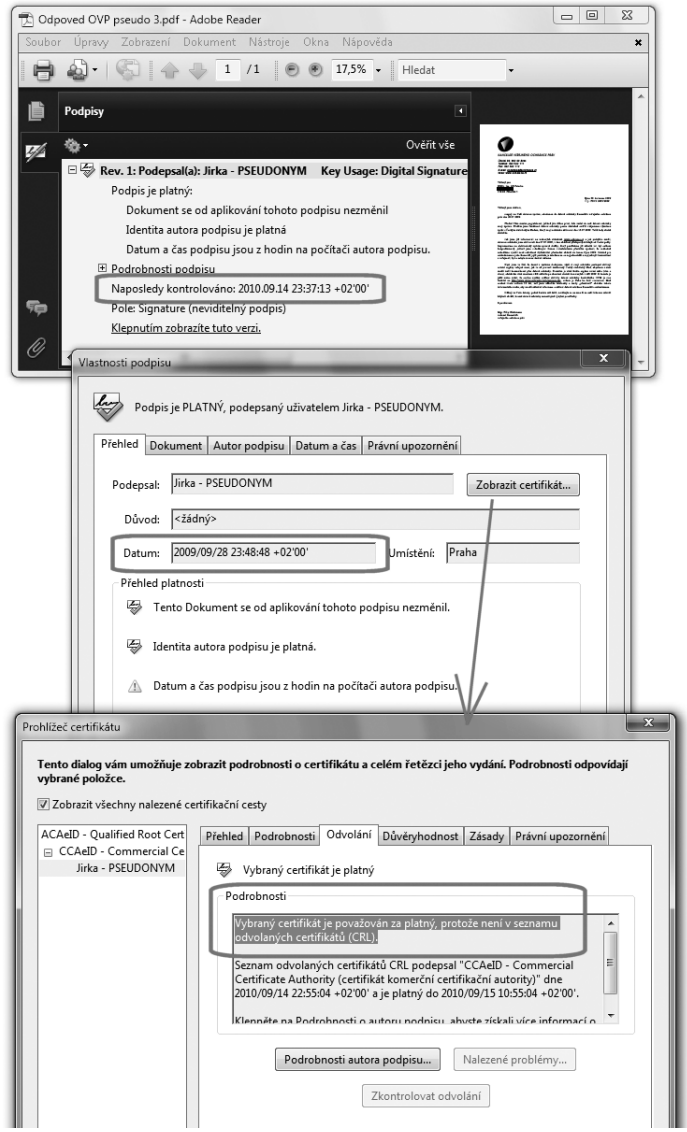
Volba posuzovaného okamžiku samozřejmě ovlivňuje i výsledek kontroly toho, zda certifikát, na kterém je podpis založen, nebyl k posuzovanému okamžiku revokován (předčasně zneplatněn).

Ukažme si to na příkladu elektronického podpisu na dokumentu, který není opatřen (podpisovým) časovým razítkem, měl být vytvořen 28. 9. 2009 (podle časového údaje přímo v podpisu), a je založen na certifikátu, který byl revokován k 21. 10. 2009. Platnost podpisu byla ověřována dne 14. 9. 2010.

Pokud bude při ověřování tohoto podpisu Adobe Reader nastaven implicitně (tj. posuzovaným okamžikem bude údajný okamžik vzniku podpisu, tj. 28. 9. 2009), bude podpis ověřen jako platný, protože úspěšně „projde“ kontrolou revokace certifikátu: k datu 28. 9. 2009 certifikát ještě nebyl revokován.

Vše ukazuje obrázek na následující stránce: jeho spodní část se odvolává na CRL seznam, aktuální v době ověřování (14. 9. 2010).

Obrázek 6-24
Zjištění, že certifikát nebyl revokován (posuzovaným okamžikem je okamžik vzniku podpisu)

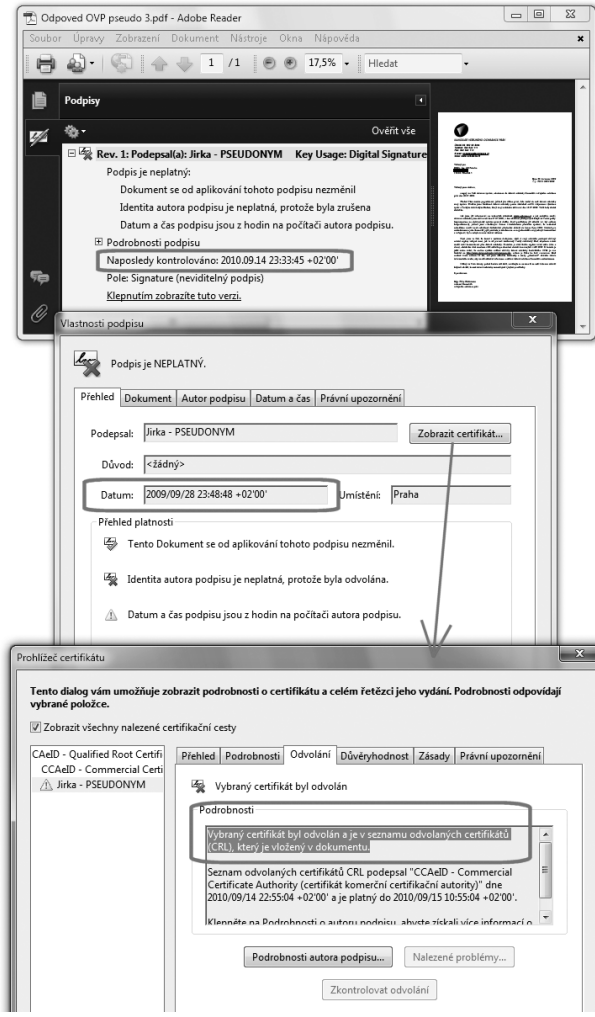


Na tomto seznamu je sice předmětný certifikát uveden, ale s datem revokace 21. 10. 2009.

Vzhledem k dřívějšímu posuzovanému okamžiku (28. 9. 2009) je proto certifikát považován za platný a nerevokovaný. Díky tomu může být také celý podpis vyhodnocen jako platný.

Pokud ale bude nastavena jedna z obou zbývající možností, bude posuzovaným okamžikem (při absenci časového razítka) aktuální časový okamžik, kdy je podpis ověřován (v daném případě 14. 9. 2010). Zde už podpis „neprojde“ kontrolou revokace certifikátu, protože se zjistí, že byl revokován (k 21. 10. 2009, a tedy k dřívějšímu okamžiku než je posuzovaný okamžik).

Obrázek 6-25
Zjištění, že certifikát byl revokován (posuzovaným okamžikem je aktuální okamžik)



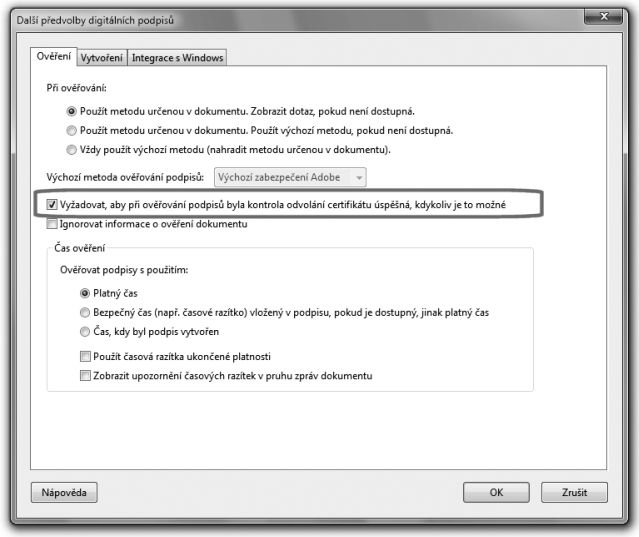
V tomto případě tedy ověření podpisu musí skončit konstatováním neplatnosti podpisu, viz obrázek.

Zdůrazněme si, že pokud by zde popisovaný PDF dokument byl opatřen časovým razítkem (resp. časový údaj u jeho podpisu pocházel z časového razítka), při nastavení na „bezpečný čas“

by posuzovaným okamžikem byl právě okamžik z časového razítka (28. 9. 2009). V té době ale certifikát revokovaný nebyl, a podpis by tak byl ověřen jako platný.

U Adobe Readeru ale musíme dávat pozor ještě na jednu věc, a tou je možnost zakázat mu (nastavením), aby prováděl kontrolu případné revokace.

Obrázek 6-26
Volba toho, zda má být kontrolována revokace



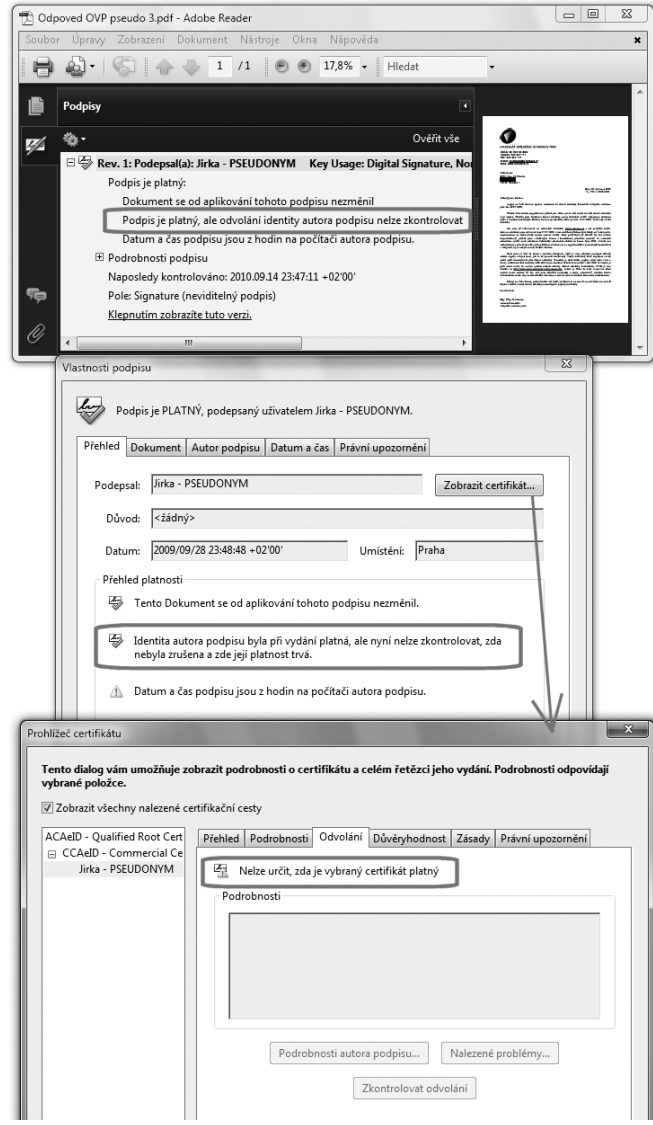
Tato volba se nastavuje hned „vedle“ nastavení posuzovaného okamžiku (viz obrázek na následující stránce, přes Úpravy, Předvolby, Zabezpečení, Další předvolby a Ověření). Pokud je tato volba zrušena, tj. pokud je nastaveno, že není požadována kontrola revokace, pak Adobe Reader prohlásí za platný i takový podpis, který by jinak (s povolenou kontrolou revokace) prohlásil za neplatný.

Příklad vidíte na obrázku na následující stránce: jde o stále stejný případ jako výše (podpis bez časového razítka měl vzniknout 28. 9. 2009, certifikát byl revokován 21. 10. 2009, ověřováno bylo 14. 9. 2010), a posuzovaný okamžik byl nastaven na aktuální (platný) okamžik.

S kontrolou revokace by tento podpis musel být ověřen jako neplatný (viz předchozí situace), ale se zakázanou kontrolou revokace jej Reader ověřil jako platný. Při detailnějším pohledu na výsledek však přeci jen lze zjistit, že revokace nebyla kontrolována – viz spodní část obrázku a záložka „Odvolání“.

Pamatujme si proto, že Adobe Reader může, ale také nemusí kontrolovat stav revokace certifikátu. Pokud jej nekontroluje, může prohlásit za platný i takový podpis, který je založen na již revokovaném certifikátu, který je tudíž neplatný. Na to, co je takovým podpisem podepsáno, se ale rozhodně nemůžeme spoléhat.

Obrázek 6-27
Ověření platnosti podpisu při zakázané kontrole stavu revokace



Naštěstí kontrola stavu revokace je v rámci implicitního nastavení požadována (příslušná volba je zaškrtnuta), takže pro správné ověřování není třeba nic měnit.

6.5.5 Kontrola revokace již expirovaného certifikátu

K pochopení toho, jak Adobe Reader ověřuje stav revokace certifikátu, se ještě musíme seznámit s jedním možným případem: představme si dokument, jehož elektronický podpis je založen na certifikátu, kterému v době ověřování již skončila jeho řádná doba platnosti (tzv. expiroval). Nicméně v době vzniku podpisu byl certifikát ještě platný – a dobu vzniku podpisu stvrzuje kvalifikované (podpisové) časové razítko, připojené k podpisu.

Takovýto podpis by stále měl být ověřen jako platný – samozřejmě pokud jsou splněny všechny další nezbytné podmínky včetně toho, že příslušný certifikát nebyl v době své řádné platnosti revokován.

Jak ale Adobe Reader zjistí, zda certifikát nebyl v době své řádné platnosti revokován? U certifikátů od tuzemských certifikačních autorit, které zatím nepodporují protokol OCSP (viz část 3.4.2), jsou jedinou možností seznamy CRL. Ty ale existují ve dvou verzích, jak jsme si již popisovali v části 3.4.4: buďto je vydáván jen jeden („kumulativní“) seznam CRL, který obsahuje i již expirované (tj. „starší“ certifikáty), nebo jsou neustále vydávány nové („intervalové“) seznamy CRL, ze kterých jsou ale vyřazovány ty certifikáty, které již expirovaly.

> Připomeňme si, že z tuzemských certifikačních autorit vydává eIdentity „kumulativní“ CRL seznam, zatímco I.CA a PostSignum vydávají „intervalové“ seznamy CRL.

Ty certifikační autority, které vydávají „intervalové“ seznamy CRL, samozřejmě zveřejňují i starší verze těchto seznamů, a to i „způsobem, umožňujícím dálkový přístup“ (přes webové rozhraní, jak jsme si také již popisovali v části 3.4.4). Problém je ale v tom, že Adobe Reader tento specifický způsob zveřejnění „starších“ verzí CRL nezná a nepodporuje, a tak se k potřebným informacím nedostane.

> Připomeňme si také, že přímo v certifikátu je uveden URL odkaz na aktuální verzi seznamu CRL. Nikoli ale již odkaz na starší verze.

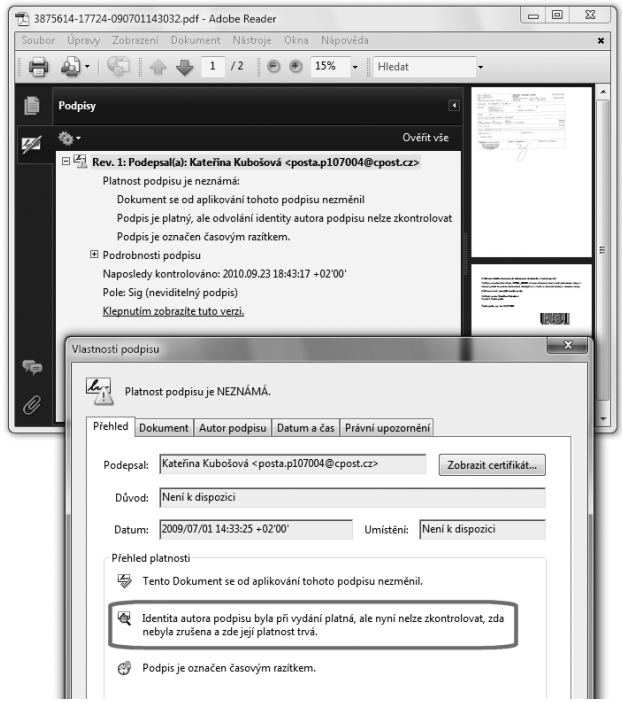
Praktické důsledky jsou tedy dosti nepříjemné: jakmile skončí řádná platnost certifikátu, na kterém je elektronický podpis založen, je vlastně jedno, zda je dokument ještě opatřen časovým razítkem či nikoli: Adobe Reader již nedokáže ověřit, zda certifikát nebyl revokován – a tak skončí verdiktem „nevím“ (resp. že platnost podpisu je neznámá).

Přesněji skončí takto u podpisů, založených na certifikátech od I.CA či PostSignum. V případě certifikátů od eIdentity revokaci ověřit dokáže.

> Zdůrazněme si, že jde o vlastnost Adobe Readeru (a jeho neschopnost získat starší verze CRL seznamů). Neznamená to, že by ověření platnosti podpisu nebylo v dané situaci možné. Jiné programy, šité na míru tuzemským certifikačním autoritám a jejich způsobu zveřejňování, si s tímto problémem mohou poradit.

Jako příklad si ukažme PDF dokument, vzniklý autorizovanou konverzí na CzechPointu přímo 1. 7. 2009 (v den, kdy došlo ke spuštění datových schránek). Jako takový je opatřen elektronickým podpisem ope-

rátora CzechPointu, založeným na certifikátu s platností od 26. 3. 2009 do 26. 3. 2010 a opatřený (podpisovým) časovým razítkem (k datu 1. 7. 2009). Ověřování probíhalo 23. 9. 2010, kdy certifikátu již skončila řádná platnost, ale časové razítko ještě bylo možné ověřit jako platné (jeho certifikátu platnost ještě neskončila). Adobe Reader byl nastaven tak, aby posuzovaným okamžikem byl okamžik vzniku podpisu (tak, jak byl zachycen časovým razítkem). Výsledkem by tedy mělo být konstatování, že podpis je platný.



Obrázek 6-28
Příklad, kdy Adobe Reader nedokázal najít informaci o revokaci certifikátu

Certifikát, na kterém je podpis založen, vydala certifikační autorita PostSignum. Ta vydává „intervalový" seznam CRL – a jelikož v době ověřování (23. 9. 2010) již skončila řádná platnost certifikátu (26. 3. 2010), na aktuálním seznamu CRL již nemohla být obsažena informace o jeho eventuální revokaci. A tak Adobe Reader skončil ověření platnosti podpisu verdiktem „nevím" – protože nedokázal najít informace o eventuální revokaci (zneplatnění).

6.5.6 Kontrola revokace podle vložených revokačních informací

Formát PDF určitým způsobem pamatuje na to, že informace o revokaci certifikátů přestávají být časem dostupné – a tak nabízí možnost vložit je přímo do samotného PDF dokumentu.

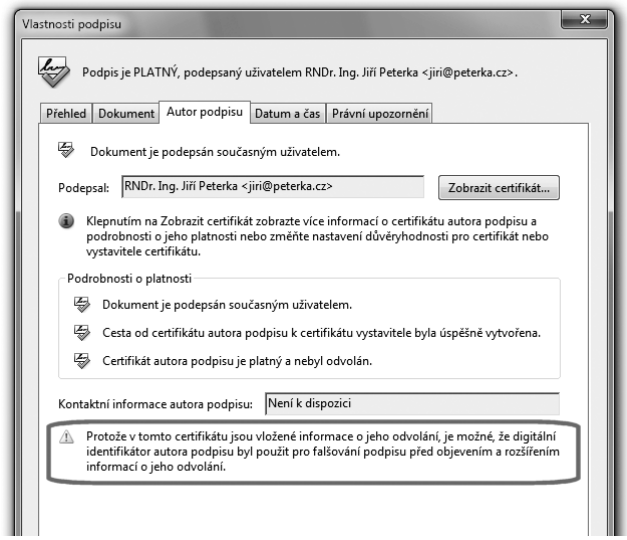
Tato možnost připadá v úvahu pro obě varianty získávání informací o revokaci, skrze protokol OCSP i skrze seznamy CRL. V prvním případě je objem vkládaných informací minimální, a tak nedochází

k významnému zvětšení souboru s PDF dokumentem. Ve druhém případě, kdy je do PDF dokumentu vkládán celý seznam CRL, může jít o velký objem dat a jeho vložením objem souboru s PDF dokumentem může značně narůst.

Samotná možnost vložení revokačních informací je dostupná ve dvou různých okamžicích: při vzniku podpisu a „později“.

První varianta ale v případě seznamů CRL neřeší daný problém, protože v okamžiku vzniku podpisu nemusí aktuální verze CRL ještě obsahovat informaci o revokaci použitého certifikátu (jelikož certifikační autority mají na zpracování žádosti a zveřejnění až 24 hodin).

Obrázek 6-29
Varování před vloženými informacemi o revokaci

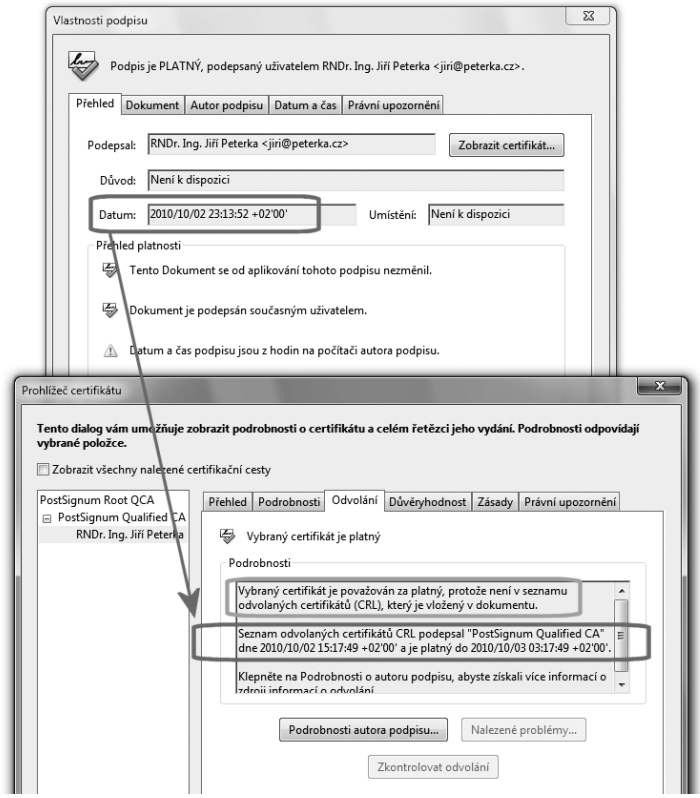


Proto i sám Adobe Reader v tomto případě varuje před tím, že vložený CRL seznam, datovaný ke stejnému okamžiku jako samotný podpis, může být prostředkem podvodu (viz předchozí obrázek).

Při ověřování podpisu je tedy nutné vždy zkontrolovat, podle jaké verze seznamu CRL bylo posuzováno případné revokování certifikátu, a zda by se na této verzi již případná revokace musela projevit či ještě nikoli.

Tuto informaci, stejně jako samotný fakt, že podpis byl ověřován podle vloženého seznamu CRL, lze získat při zobrazení informací o odvolání certifikátu, na kterém je ověřovaný podpis založen, viz následující obrázek.

> Na obrázku je situace, kdy byl do PDF dokumentu vložen „příliš mladý“ seznam CRL, který ještě nemusel obsahovat informace o případné revokaci toho certifikátu, na kterém je podpis založen.



Obrázek 6-30
Informace o hodnocení certifikátu oproti vloženému seznamu CRL (zeleně) a o datování tohoto seznamu a době vzniku podpisu (červeně)

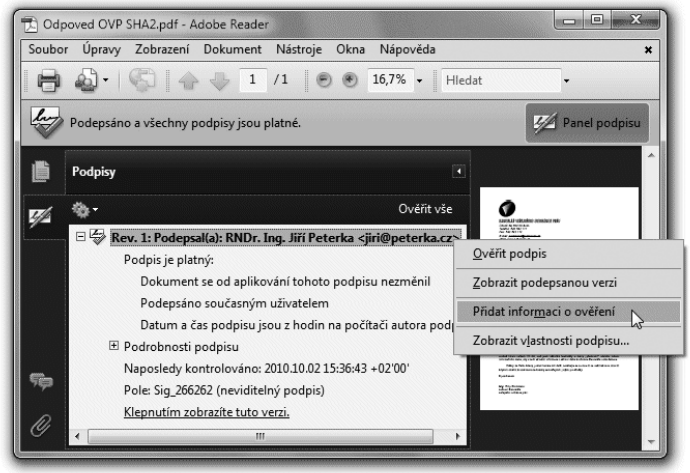
Druhá varianta vložení revokačních informací, a to „někdy později“, je podporována od verze 9.2 programu Adobe Reader (i Acrobat). V případě CRL seznamů umožňuje počkat, až bude vydán takový seznam, který by informace o revokaci již musel obsahovat. Tím se řeší výše popsaný problém. Současně ale přináší ještě jednu užitečnou možnost: aby revokační informace k podepsanému PDF dokumentu přidal někdo jiný, než podepisující osoba. Protože první varianta (vkládání revokačních informací v okamžiku vzniku podpisu) je již ze své podstaty dostupná právě jen pro podepisující osobu.

Samotné vložení informací o revokaci (seznamu CRL či odpovědi od OCSP serveru) podle první varianty, neboli při vzniku podpisu, provádí Adobe Reader (či Acrobat) sám a automaticky – ovšem jen pokud je tak nastaven. Konkrétní postup nastavení si ukážeme v části 6.11.3.[8]

Vložení revokačních informací podle druhé varianty, neboli do již podepsaného PDF dokumentu, může iniciovat sám uživatel, který s dokumentem právě pracuje a ověřuje platnost podpisů.

[8] Od verze 9.2 programů Reader a Acrobat je vkládání revokačních informací „při vzniku podpisu“ implicitně zapnuto, zatímco ve verzi 9.1 bylo ještě vypnuto.

Obrázek 6-31
Nabídka vložení informací o revokaci



V případě úspěšného ověření je mu nabídnuta možnost vložit do PDF dokumentu ty revokační informace, které byly v rámci právě provedeného ověření získány.

Postup naznačuje obrázek, volbou nabídky dostupné přes pravé tlačítko. V případě Adobe Readeru se ale takovéto vložení skutečně provede jen tehdy, pokud je příslušný PDF dokument tzv. odemknut (aktivován) pro podepisování a další změny, viz část 6.10.

6.5.7 Kontrola řádné doby platnosti certifikátu

Kromě ověření integrity podepsaného dokumentu a kontroly revokace certifikátu, na kterém je podpis založen, program Adobe Reader samozřejmě zkoumá také řádnou dobu platnosti tohoto certifikátu.

Pokud zjistí, že k posuzovanému okamžiku již skončila, nedokáže již pokračovat v ověřování platnosti podpisu a musí skončit konstatováním, že je neznámá. Důvodem je to, že se již nemůže spoléhat na platnost údajů, obsažených v certifikátu. Pro posuzování řádné doby platnosti certifikátu nemá Adobe Reader žádné nastavení, které by ovlivňovalo tuto jeho činnost.

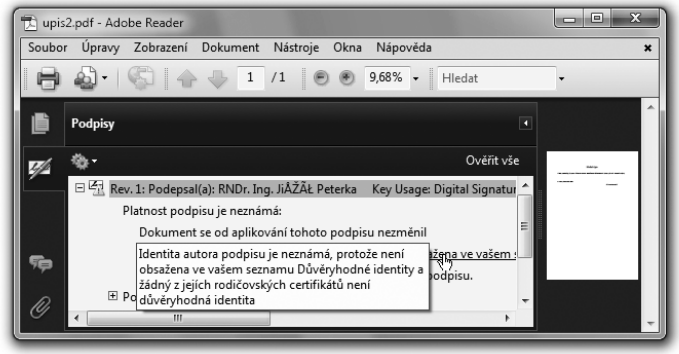
6.5.8 Platnost nadřazených certifikátů

Kromě toho certifikátu, na kterém je právě ověřovaný podpis založen, musí Adobe Reader zkoumat i všechny jemu nadřazené certifikáty (na příslušné certifikační cestě). U všech musí ověřit, zda k posuzovanému okamžiku nebyly revokovány,[9] a také zda již neskončila jejich řádná platnost.

[9] S výjimkou kořenového certifikátu, jehož revokaci Reader neověřuje. Musel by vycházet z revokačních údajů, podepsaných s využitím toho samého certifikátu, na jehož revokaci se právě ptá. Pokud k revokaci došlo, nemohl by údajům o ní věřit.

Případné důsledky jsou obecně stejné, jako u „výchozího“ certifikátu, na kterém je založen právě ověřovaný podpis: pokud by některý z nadřazených certifikátů byl k posuzovanému okamžiku revokován, musí být ověřovaný podpis prohlášen za neplatný. Jinak pokud by některému nadřazenému certifikátu skončila jeho řádná platnost, muselo by ověřování platnosti podpisu skončit výsledkem „nevím“, resp. „platnost podpisu je neznámá“.

Obrázek 6-32
Adobe Reader nedokáže najít (platné) nadřazené certifikáty



Kontrolu stavu revokace a řádné doby platnosti všech nadřazených certifikátů provádí Adobe Reader sám a automaticky, jako součást ověřování zkoumaného podpisu. Uživatel by o tom v zásadě ani nemusel vědět.

Přesto je zde jedno úskalí, které musí vyřešit uživatel: musí zajistit, aby program Adobe Reader měl přístup ke všem nadřazeným certifikátům na certifikační cestě. Protože pokud se tak nestane a některý z nadřazených certifikátů nebude k dispozici, Reader skončí s verdiktem, že platnost certifikátu je neznámá. Protože ji skutečně nedokáže ověřit.

Sám Adobe Reader ovšem takovouto situaci formuluje poněkud komplikovaněji a pomocí jiné terminologie, když místo o tom certifikátu, na kterém je podpis založen, hovoří o „identitě autora podpisu“ (která „není obsažena v uživatelově seznamu důvěryhodných identit“), a místo o nadřazených certifikátech hovoří o „rodičovských certifikátech, které nejsou důvěryhodnými identitami“, viz předchozí obrázek.

6.5.9 Úložiště certifikátů

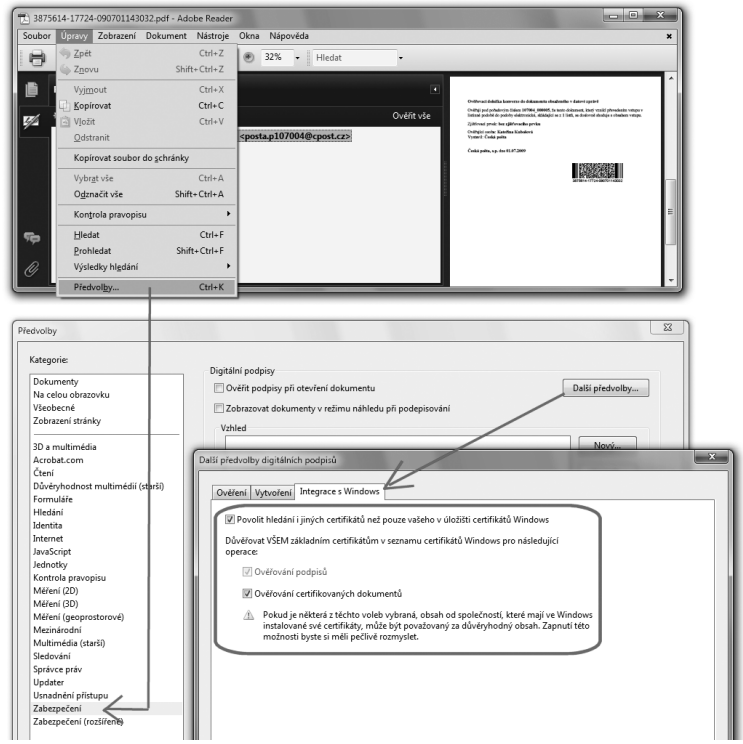
K tomu, aby se Adobe Reader vůbec zabýval nadřazenými certifikáty, jejich pouhá dostupnost nestačí. Ještě je zapotřebí, aby Adobe Reader měl důvod považovat je za důvěryhodné. Teprve pak je začne zkoumat, zda nebyly revokovány a zda ještě neskončila jejich řádná platnost.

Jak již víme z předchozích částí této knihy, vyjádření důvěry v certifikát (a současně s tím i jeho zpřístupnění) se provede uložením certifikátu do správné části toho úložiště (důvěryhodných) certifikátů, se kterým Adobe Reader právě pracuje.

V této souvislosti si připomeňme, že Adobe Reader dokáže pracovat se dvěma úložišti certifikátů: se svým vlastním a se systémovým úložištěm MS Windows.

> Přesněji je to ale tak, že Reader pracuje buďto jen se svým vlastním úložištěm, nebo s oběma úložišti současně (s jejich logickým sjednocením). Tedy jakoby si k obsahu svého vlastního úložiště přidal obsah systémového úložiště v MS Windows. V terminologii jeho uživatelského rozhraní je to označováno jako „Integrace s Windows".

Implicitně (bezprostředně po své instalaci) přitom Adobe Reader používá první variantu, neboli pracuje jen s obsahem svého úložiště. Druhou variantu lze aktivovat postupem, který ukazuje obrázek.



Obrázek 6-33
Postup nastavení programu Adobe Reader tak, aby využíval i systémové úložiště MS Windows

Obecně přitom platí, že za správné naplnění toho úložiště, které Adobe Reader používá, odpovídáme my uživatelé. I proto bychom měli znát nejenom to, jak se chová systémové úložiště certifikátů v MS Windows, ale také to, že vlastní úložiště Readeru má určitou „počáteční výbavu", určité mechanismy pro automatické načítání certifikátů, a také přeci jen určité vnitřní strukturování: musíme mu sami říci, které certifikáty má považovat za kořenové. Podrobněji viz části 5.4.2.1 a 5.4.3.3.

6.5.10 Jaké certifikáty zařadit mezi důvěryhodné?

Upřesněme si ještě jednou, že když Adobe Reader bude vyhodnocovat nějaký konkrétní podpis, bude se snažit zjistit, zda je tento podpis založen na takovém certifikátu, který může považovat za důvěryhodný, a stejně tak všechny jemu nadřazené certifikáty na příslušné certifikační cestě. Pouze v tomto případě (a při splnění všech ostatních podmínek) bude moci prohlásit podpis za platný.

Důvěryhodnost každého konkrétního certifikátu přitom posuzuje podle toho, zda se přímo tento certifikát nachází v úložišti důvěryhodných certifikátů, nebo zda se zde nachází jemu nadřazený certifikát, neboli certifikát příslušného vydavatele (certifikační autority).

Jak již také víme, vyjadřovat důvěru individuálně jednotlivým „podpisovým" certifikátům by mělo být spíše výjimkou potvrzující obecné pravidlo, že důvěra se vyjadřuje vydavatelům certifikátů (certifikačním autoritám), a do úložišť jsou ukládány především jejich certifikáty. Připomeňme si také, že certifikáty certifikačních autorit se do příslušného úložiště mohou dostat různými způsoby: jako jejich „počáteční náplň", skrze mechanismy pro automatickou instalaci certifikátů nebo „ručně", samotnými uživateli či správci (viz část 5.4).

V našich zeměpisných šířkách by tak v úložišti měly být všechny kořenové certifikáty všech tuzemských akreditovaných certifikačních autorit (tj. I.CA, Postsignum a eIdentity), a také certifikáty všech jejich podřízených (zprostředkujících) autorit, které vydávají kvalifikované certifikáty (jak jsme si popisovali již v části 1.10).

S takto nastaveným obsahem úložiště certifikátů (obsahujícím kořenové certifikáty a certifikáty kvalifikovaných podřízených autorit) pak bude korektně ověřována platnost uznávaných elektronických podpisů, uznávaných značek a kvalifikovaných časových razítek, založených na certifikátech tuzemských certifikačních autorit. Mějme ale na paměti, že dnes již jsou za uznávané považovány i takové elektronické podpisy, které jsou založené na kvalifikovaných certifikátech některých zahraničních certifikačních autorit (podrobněji viz seznamy TSL, část 4.5.3).

Samozřejmě můžeme do příslušného úložiště sami přidat také certifikáty dalších vydavatelů (certifikačních autorit), které považujeme za důvěryhodné – tak, aby i podpisy založené na jimi vydaných certifikátech mohly být vyhodnoceny jako platné. Například chceme-li, aby se korektně vyhodnocovaly podpisy založené na komerčních certifikátech (byť nebudou „uznávané"), musíme do právě používaného úložiště nainstalovat také certifikáty příslušných (komerčních) certifikačních autorit. Například certifikačních autorit našich obchodních partnerů či (podřízených) komerčních autorit akreditovaných autorit, jako je PostSignum, eIdentity či I.CA.

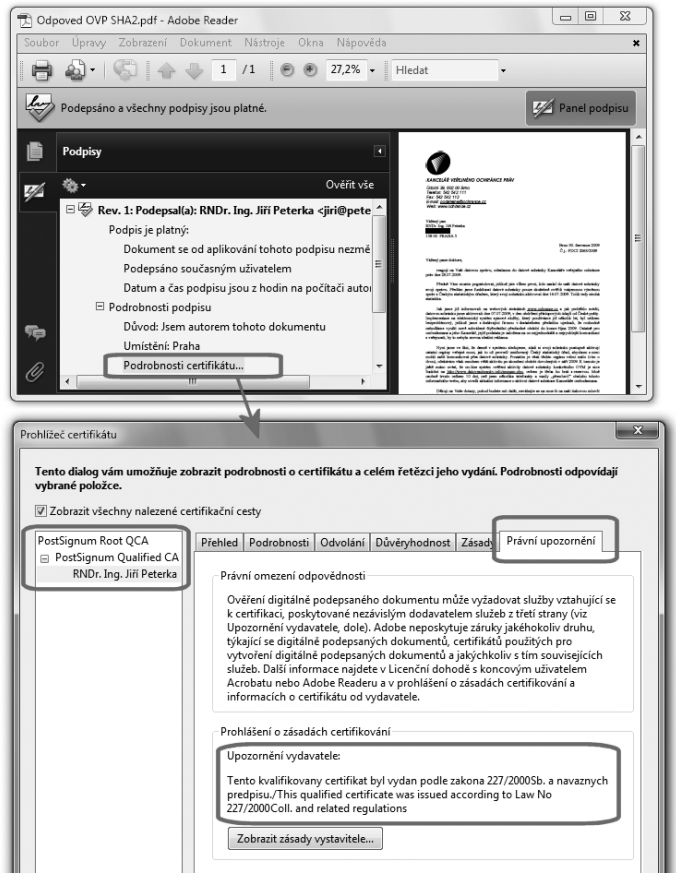
6.5.11 Jak poznat uznávaný podpis?

I v souvislosti s předchozím odstavcem si znovu připomeňme, že program Adobe Reader nám při ověřování podpisu vůbec neřekne, zda jde o platný uznávaný elektronický podpis, platný zaručený elektronický podpis či třeba platnou elektronickou značku. Řekne nám jen to, že „podpis je platný" (případně „je neplatný" či „nevím") – ale již nám neřekne, o jaký druh podpisu se jedná.

Je to dáno tím, že Adobe Reader (stejně jako většina ostatních programů) vlastně vůbec nerozlišuje jednotlivé varianty elektronických podpisů tak, jak je zná a rozlišuje náš právní řád. Nezkoumá totiž „kvalitu“ certifikátu, na kterém je podpis založen: nerozlišuje, zda jde třeba jen o nějaký testovací certifikát či certifikát komerční, nebo zda jde o certifikát kvalifikovaný.

Stejně tak Reader nerozlišuje ani „původ“ certifikátu: zda byl vydán akreditovanou certifikační autoritou, nebo certifikační autoritou bez akreditace, nebo zda si jej třeba někdo vydal sám sobě, jakoby „na koleně“. Viz diskuse v části 4.5.1.

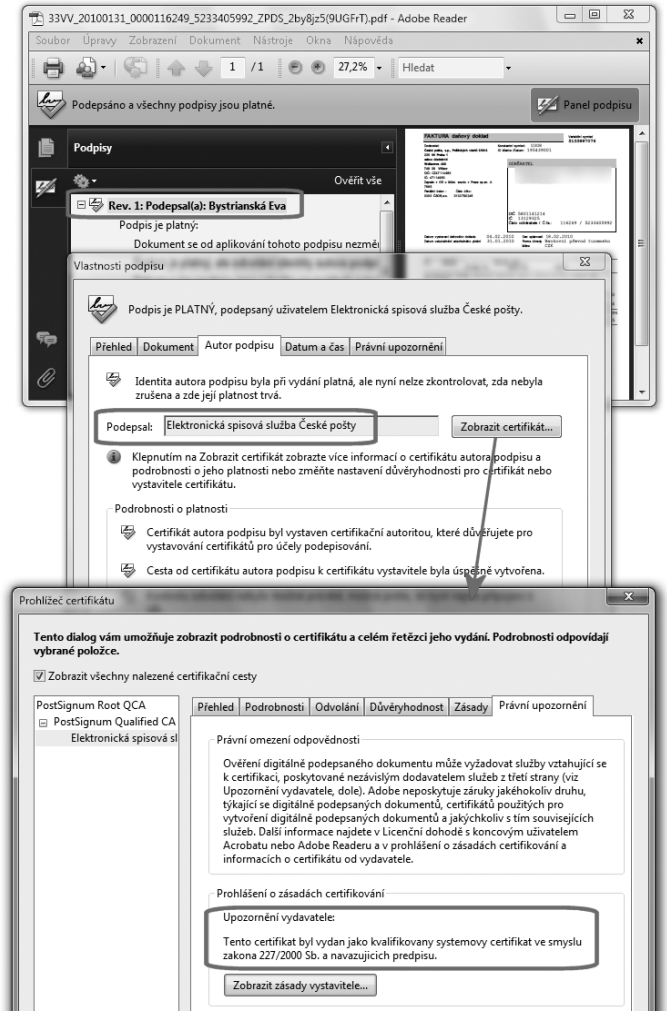
To jediné, co Reader v souvislosti s „kvalitou“ certifikátů zajímá je, zda konkrétní certifikát může považovat za důvěryhodný. A to odvozuje výlučně od toho, zda je příslušný certifikát obsažen v právě používaném úložišti (důvěryhodných) certifikátů, viz výše. Břímě posuzování kvality a původu certifikátu – a s tím i rozlišování druhu elektronického podpisu – tak fakticky přenáší na toho, kdo mu toto úložiště naplňuje.



Obrázek 6-34
Příklad zjištění, že jde o uznávaný elektronický podpis

Je tedy na nás, uživatelích programu Adobe Reader, abychom si sami zjistili, o jaký druh elektronického podpisu na PDF dokumentu se jedná, případně zda se nejedná o elektronickou značku (a jakou).

Vše přitom zjistíme z certifikátu, na kterém je ověřovaný podpis založen. Musíme jej ale prozkoumat a správně zhodnotit sami. Po věcné stránce to naštěstí není nijak těžké: necháme si příslušný certifikát zobrazit, a pak jej hodnotíme. V případě kvalifikovaných certifikátů od tuzemských certifikačních autorit to máme nejjednodušší: musí to mít v sobě napsáno. A tak hledáme příslušnou poznámku (buďto v položce „zásady certifikátu“, nebo přes „prohlášení“ vydavatele).



Obrázek 6-35
Příklad zjištění, že jde o uznávanou elektronickou značku

V případě uznávaných elektronických podpisů ale musíme ověřit ještě jejich druhou podmínku: zda kvalifikovaný certifikát byl vystaven akreditovanou certifikační autoritou (akreditovaným poskytovatelem certifikačních služeb).

Pokud to není automaticky splněno tím, že všichni vydavatelé kvalifikovaných certifikátů jsou akreditovaní (což byla situace v ČR v době vzniku této knihy, v roce 2010), pak je nutné nejprve zjistit, kdo je vydavatelem certifikátu (podle nadřazených certifikátů na certifikační cestě) a pak ověřit, zda tento vydavatel má na vydávání kvalifikovaných certifikátů akreditaci.

> Připomeňme si, že u certifikátů vydaných zahraničními vydavateli (z EU) je situace složitější (viz část 4.5.3) a je třeba konzultovat seznamy TSL.

Stejně tak je ale na nás uživatelích, abychom rozpoznali, zda podpis na PDF dokumentu není ve skutečnosti uznávanou elektronickou značkou (viz část 4.6.1). To opět poznáme podle toho, na jakém certifikátu je založen. V případě elektronické značky jde o kvalifikovaný systémový certifikát.

Právě v případě značky se také nenechme zmást tím, že Adobe Reader nám jako podepsanou (resp. označující) osobu může uvádět někoho jiného (nejspíše nějakého operátora, resp. operátorku) a nikoli toho, komu byl kvalifikovaný systémový certifikát vystaven. Což dále ztěžuje rozlišení elektronické značky od elektronického podpisu.

Podobný „úkaz“, byť v souvislosti s elektronickými podpisy, jsme si ukazovali v části 6.6.1.

6.5.12 Jak poznat kvalifikované časové razítko

Jak jsme si již uvedli výše, časová razítka nejsou u PDF dokumentů chápána jako „samostatná“, ale jen jako atribut časového údaje na konkrétním elektronickém podpisu (jako „podpisová“ časová razítka).[10]

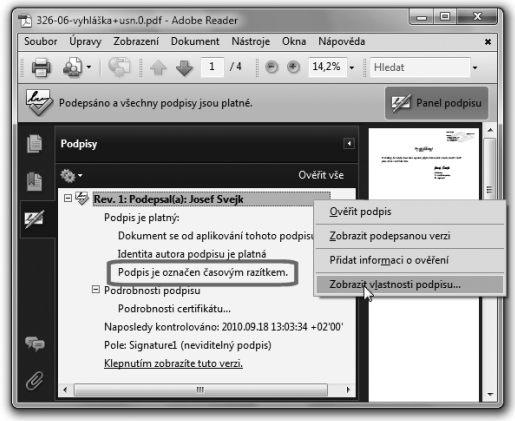
O tom, že dokument je opatřen časovým razítkem (přesněji: že konkrétní elektronický podpis či značka je doplněn časovým razítkem) se dozvíme jen z poznámky u konkrétního podpisu, viz následující obrázek.

Stejně jako u samotného podpisu již ale Adobe Reader nezkoumá, o jaký druh časového razítka se jedná: zda o „obyčejné“ časové razítko, nebo o časové razítko kvalifikované, pocházející od kvalifikované certifikační autority (na které se již můžeme spoléhat).

---

[10] Odlišná jsou „archivní“ časová razítka, popisovaná v části 6.11. I pro ně ale platí vše, co je uvedeno v této části ohledně rozpoznávání druhu časového razítka.

Obrázek 6-36
Jak se dostat k údajům o časovém razítku – přes vlastnosti podpisu



Zjištění, o jaký druh (podpisového) časového razítka se jedná, je opět na nás uživatelích. Ukažme si proto možný postup na obrázcích.

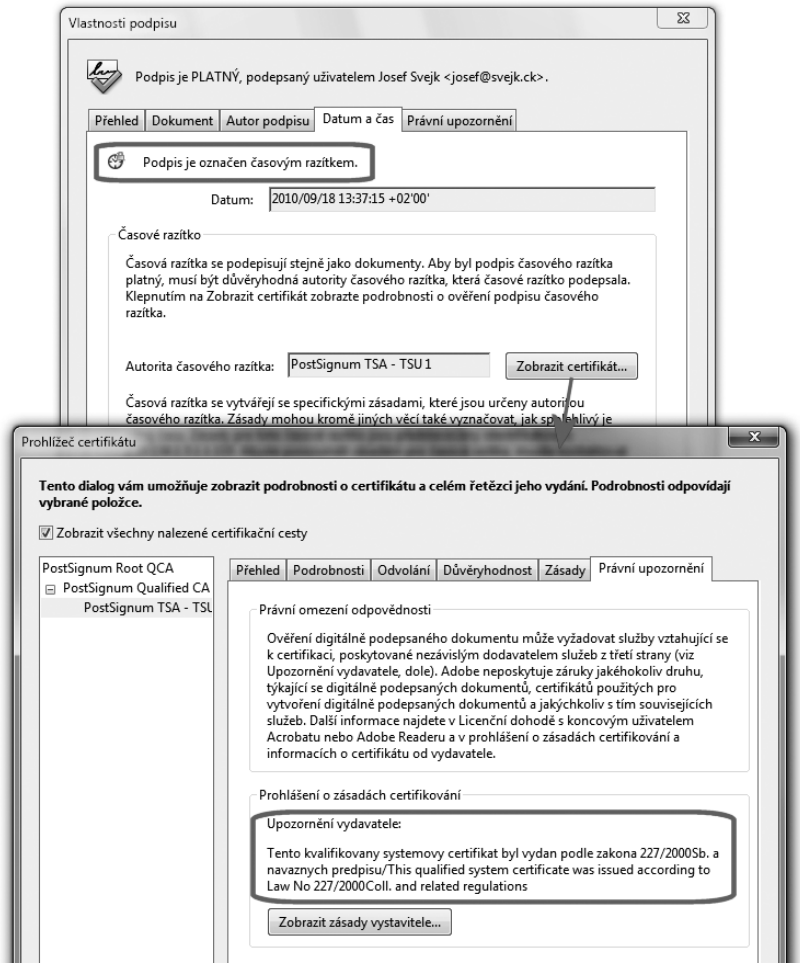
První obrázek (na této stránce) ukazuje samotné konstatování, že podpis na PDF dokumentu je opatřen (podpisovým) časovým razítkem, viz červený rámeček. Dále naznačuje, jak se dostat k bližším údajům o časovém razítku: je třeba si nechat zobrazit detaily samotného podpisu (a nesnažit se získat detaily časového razítka, tudy cesta nevede).

Když již Adobe Reader zobrazuje podrobnosti podpisu, je třeba se podívat na záložku s údaji o datu a čase. Zde již je uveden časový okamžik, obsažený na časovém razítku. Dále je uveden jeho vydavatel a je možné si nechat zobrazit certifikát, na kterém je založeno (podpisové) časové razítko. Teprve podle tohoto certifikátu poznáme, zda jde o kvalifikované časové razítko (které musí být založeno na kvalifikovaném systémovém certifikátu), nebo nikoli.

Při zkoumání časových razítek bychom měli mít na paměti také to, že druh podpisu a druh časového razítka jsou na sobě zcela nezávislé. Můžeme mít PDF dokument s uznávaným elektronickým podpisem, který je opatřen takovým (podpisovým) časovým razítkem, které není kvalifikované. A naopak: můžeme mít PDF dokument opatřený pouze zaručeným (nikoli uznávaným) elektronickým podpisem, ale opatřený kvalifikovaným časovým razítkem.

Příklad, který vidíte na předchozím i následujícím obrázku, je právě druhého typu: jde pouze o zaručený (nikoli uznávaný) podpis literární postavy Josefa Švejka, opatřený kvalifikovaným (podpisovým) časovým razítkem.

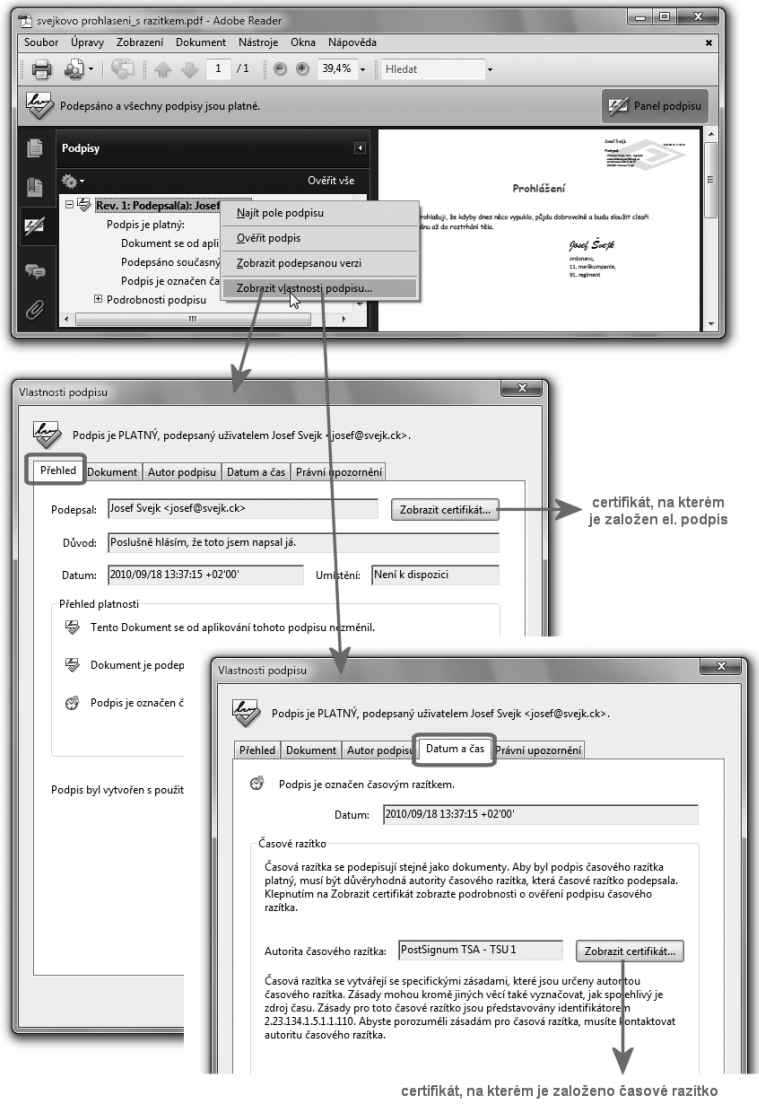
Obrázek 6-37
Příklad zobrazení certifikátu, na kterémje založeno časové razítko na PDF



Pamatujme na odlišnost podpisu a razítka i při jejich praktickém zkoumání. O to více, že program Adobe Reader nám zde klade určité nástrahy tím, že (podpisové) časové razítko chápe jako nesamostatné, jako atribut podpisu: k oběma certifikátům se dostaneme stejnou cestou, přes vlastnosti podpisu.

A to přímo svádí k tomu, abychom si oba certifikáty popletli. Rozdíl by měl vyplývat z předchozích obrázků, ale pro jistotu si jej ještě jednou zdůrazněme skrze následující obrázek.

Obrázek 6-38
Rozlišení certifikátů, na kterých je založen podpis a časové razítko



6.6 Ověřování interních podpisů jinými programy

Volně šiřitelný program Adobe Reader samozřejmě není jediným možným nástrojem pro ověřování elektronických podpisů, značek a časových razítek na PDF dokumentech. V praxi je možná nejpoužívanější, ale rozhodně není jedinou alternativou.

Vedle něj existují i další alternativy, které si můžeme rozdělit do dvou kategorií, na:

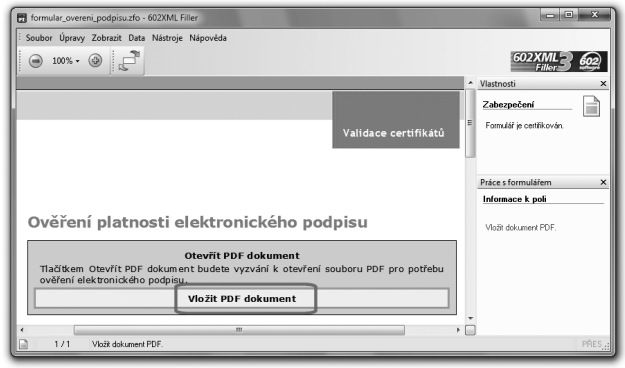
- programy (které si uživatel musí instalovat na svém počítači a pak spouštět)
- on-line služby (dostupné na Internetu, neinstalují se, ale rovnou používají)

Dalším zásadním rozdílem mezi nimi je to, že u programů má jejich nastavení na starosti uživatel, zatímco u on-line služeb je nastavuje jejich provozovatel. Na to je třeba pamatovat i s ohledem na to, které kořenové certifikáty jsou tím kterým nástrojem považovány za důvěryhodné a které nikoli.

Příkladem programu, který může uživatel využít pro ověřování platnosti elektronických podpisů, je program VerisignIT od české společnosti Dignita. Ten si podrobněji představíme v následujících odstavcích jako program, který umožňuje ověřovat i externí elektronické podpisy. Vedle nich samozřejmě umožňuje ověřovat i podpisy interní, a také tyto podpisy vytvářet.

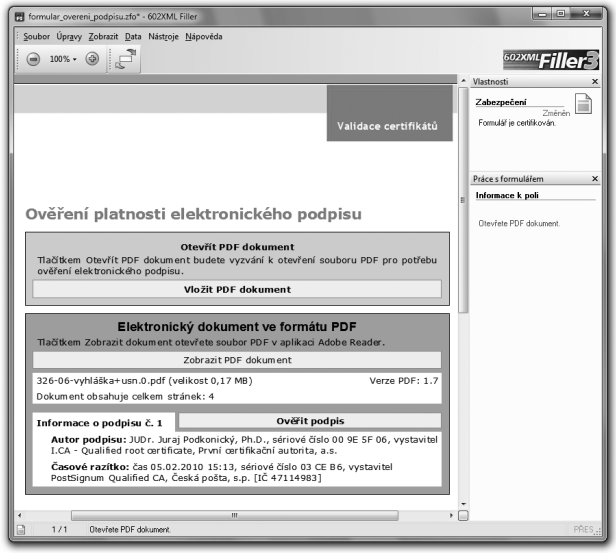
Příkladem on-line služby pro ověřování interních podpisů na PDF dokumentech může být služba dostupná na serveru BEZPAPIRU.CZ, konkrétně na adrese *http://www.bezpapiru.cz/overovani*. Fakticky jde o formulář ve formátu ZFO, který si můžete stáhnout na svůj počítač a zde otevřít v programu 602XML Filler.

Obrázek 6-39
Ověřovací formulář v 602XML Filleru



Prostřednictvím tohoto formuláře pak vyberete soubor s PDF dokumentem, který chcete ověřit. Ten je formulářem načten a jsou vám zobrazeny základní údaje o tom, zda je dokument podepsán a opatřen časovým razítkem, plus údaje obsažené v příslušných certifikátech (komu patří podpisový certifikát, kdo vydal časové razítko atd.).

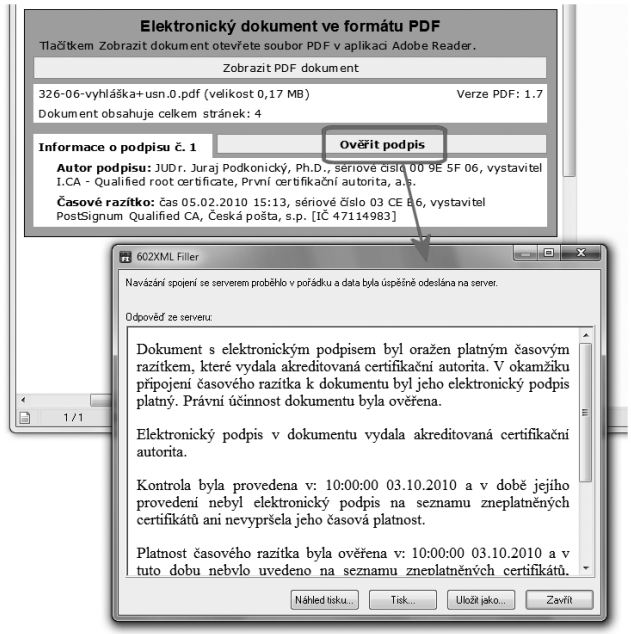
Obrázek 6-40
Zobrazení informací o podpisu a razítku na PDF dokumentu



Všechny tyto činnosti přitom probíhají „na počítači“ a nikoli on-line.

Teprve po kliknutí na volbu „Ověřit podpis“ je využita on-line služba: otisk PDF dokumentu je odeslán na server, který vyhodnotí jeho podpis, značku a razítko, a o výsledku informuje uživatele v novém okně, viz obrázek na následující stránce.

Obrázek 6-41
Příklad výsledku ověření



Důležitým rozdílem této varianty (oproti použití „místního“ programu), je otázka důvěryhodnosti certifikátů: v případě „místního“ programu je důvěryhodnost odvozována od obsahu toho úložiště důvěryhodných certifikátů, se kterým program právě pracuje. V případě on-line služby je tato důvěryhodnost dána nastavením služby a tedy tím, které certifikáty považuje za důvěryhodné provozovatel služby.

> V konkrétním případě služby, kterou poskytuje server BEZPAPIRU CZ, by mělo jít o stejné nastavení důvěryhodnosti, jaké používají kontaktní místa CzechPointů. Lze si představit, že tato služba sdílí s CzechPointy společné úložiště důvěryhodných certifikátů.

6.7 Ověřování externích elektronických podpisů na PDF dokumentech

V praxi se kromě interních elektronických podpisů, značek a časových razítek („vložených“ přímo do příslušného dokumentu) můžeme setkat i s podpisy (a časovými razítky) externími, které jsou obsaženy v samostatných souborech.

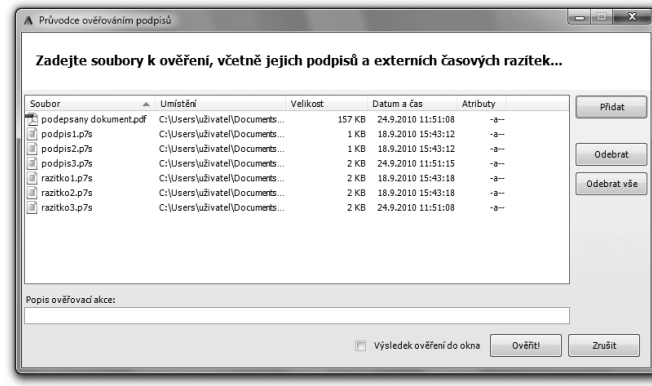
Jejich nespornou výhodou je to, že jimi lze podepsat (či: označit a také opatřit časovým razítkem) jakýkoli dokument a nikoli jen PDF dokument. Obecně jakýkoli soubor, nejenom soubor obsahující dokument. Třeba i takový soubor, který vůbec nepodporuje interní elektronické podpisy.

> Další odstavce se tedy mohou vztahovat k ověřování externích podpisů (značek a razítek) obecně, a ne pouze k dokumentům v souborech formátu PDF (PDF dokumentům).

K ověřování externích podpisů, značek a razítek samozřejmě potřebujeme takové prostředky, které tuto funkčnost podporují. Mezi ně ale již nepatří program Adobe Reader, který pracuje pouze s interními podpisy.

Zde si ověřování externích podpisů, značek a razítek ukážeme na příkladu programu VerisignIT od společnosti Dignita. Princip by nicméně měl být v zásadě stejný u všech programů, které s externími podpisy dokáží pracovat.

Obrázek 6-42
Volba podepsaného souboru a souborů s externími podpisy a časovými razítky



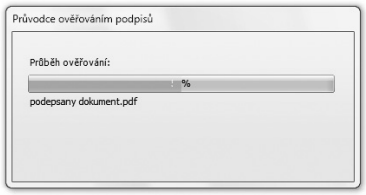
V prvním kroku je třeba ověřujícímu programu zadat konkrétní soubory, které obsahují samotný „podepsaný“ soubor, a dále soubory, obsahující podpisy, značky a razítka. Těch může být více, protože stejně jako v případě interních podpisů může být jeden a tentýž soubor opatřen více externími podpisy, značkami a razítky.

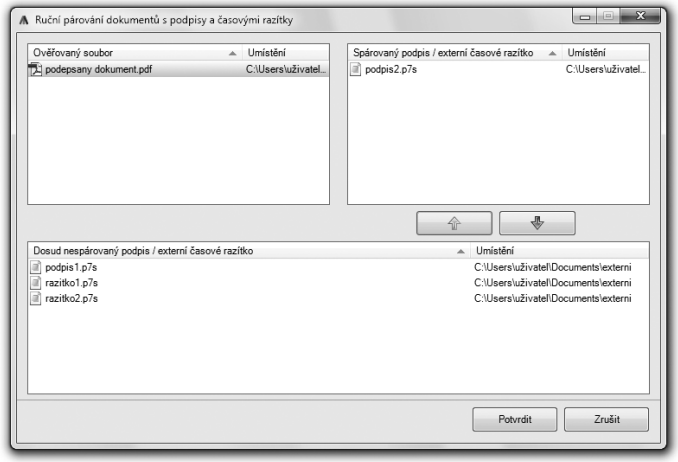
Výběrem souborů, obsahujících externí podpisy, značky a razítka uživatel jakoby „nahrubo“ specifikuje vazbu mezi tím, co je podepsaný soubor a co je jeho podpis, značka či časové razítko. Programu pro ověřování to může stačit: projde uvedené soubory, podle jejich typů (přípon) si domyslí co obsahují – a snaží se vydedukovat, který podpis patří ke kterému souboru. To pozná hlavně při zkoumání integrity podepsaného souboru.

Samozřejmě se ale může stát, že ověřujícímu programu se nepodaří správně „spárovat“ podepsaný soubor s jeho podpisy, značkami a razítky. Pak mu nezbývá, než si vyžádat spolupráci uživatele a požadované spárování chtít od něj. Příklad takovéto situace ukazuje první obrázek na následující stránce.

Obrázek 6-43

Příklad ručního párování dokumentu s externím podpisem a časovým razítkem

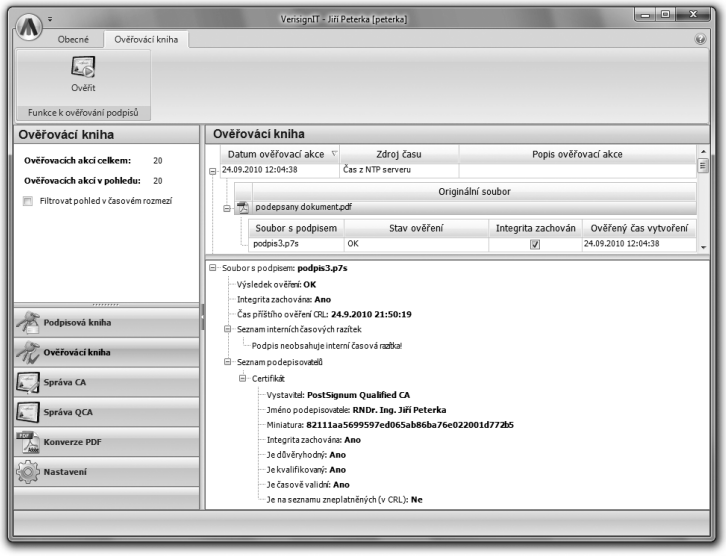




Jakmile je dosaženo potřebného spárování podepsaného souboru s jeho podpisy, značkami a razítky, je již na ověřujícím programu, aby ověření provedl a oznámil výsledek. Příklad toho, jak to činí program VerisignIT, vidíte na následujícím obrázku.

Obrázek 6-44

Výsledek ověření externího el. podpisu



6.8 Podepisování PDF dokumentů nástroji třetích stran

Pro podepisování PDF dokumentů (přidávání elektronických podpisů či značek, a také časových razítek) existuje celá řada programů a utilit jak od společnosti Adobe, tak i od třetích stran. Zde se nejprve seznámíme s řešeními od třetích stran (a v další části i s možnostmi, které nabízí produkty Adobe).

Obecně pro podepisování existují dvě základní možnosti:

- podepsání (a přidání „podpisového" časového razítka) při vytváření PDF dokumentu
- přidání podpisu (a razítka) k již existujícímu PDF dokumentu

První varianta se týká situací, kdy PDF dokument teprve vzniká, a to nejčastěji skrze konverzi z nějakého jiného datového formátu. Příslušný konverzní program, je-li k tomu uzpůsoben, může ke vznikajícímu PDF dokumentu rovnou připojit i jeho podpis. Snad vždy je ale tato možnost omezena jen na jeden elektronický podpis.

Ze všech konverzních programů, schopných vytvářet PDF dokumenty, ale mají schopnost připojit elektronický podpis jen některé. A z nich opět jen některé jsou schopny přidat k podpisu také (podpisové) časové razítko.

Přidat k jednomu dokumentu více elektronických podpisů umožňuje obvykle až druhá varianta, při které příslušný program (pro podepisování) manipuluje s již existujícím PDF dokumentem. Pak není problémem přidat k jednomu PDF dokumentu tolik elektronických podpisů (či značek), kolik je třeba. A to buď najednou, v rámci jedné operace, ale častěji spíše opakovaně (opakovaným použitím podepisujícího programu těmi osobami, které k dokumentu připojují svůj podpis).

Ty programy, které mají schopnost připojit k již existujícímu PDF dokumentu elektronický podpis (případně značku), se mohou dále lišit i v rozsahu této své schopnosti. Některé například dokáží vytvářet jen neviditelné podpisy (viz část 6.1). Jiné zvládají i podpisy viditelné, a nabízí třeba i možnost vytvářet různé varianty jejich vzhledu.

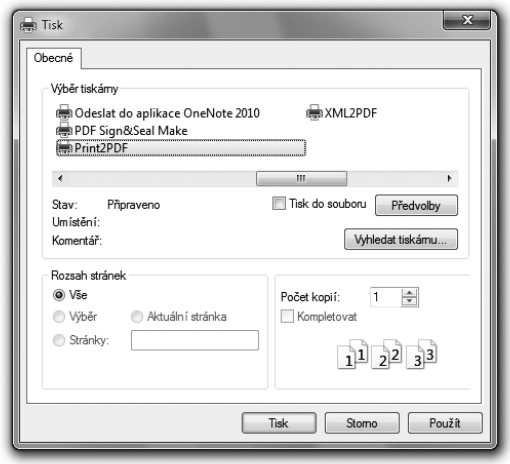
Podobně jen některé z programů, schopných přidávat elektronický podpis, zvládnou přidat také časové razítko.

6.8.1 Virtuální PDF tiskárny

Programy, používané pro konverzi dokumentů do formátu PDF, mají velmi často podobu virtuální tiskárny. To znamená, že do operačního systému počítače nainstalují ovladač, který uživateli vytváří iluzi nové tiskárny. Jen místo „na papír" tiskne „do PDF dokumentu": výsledkem tisku je nový PDF dokument, který si uživatel uloží tam, kam chce.

Výhodou této varianty je možnost konvertovat do PDF prakticky jakýkoli zdrojový formát: stačí, aby program, který s výchozím formátem pracuje, uměl tisknout. Pak již stačí jen zvolit příslušnou „PDF tiskárnu“ a nechat tisk proběhnout.

Obrázek 6-45
Příklad nabídky virtuální PDF tiskárny v MS Windows

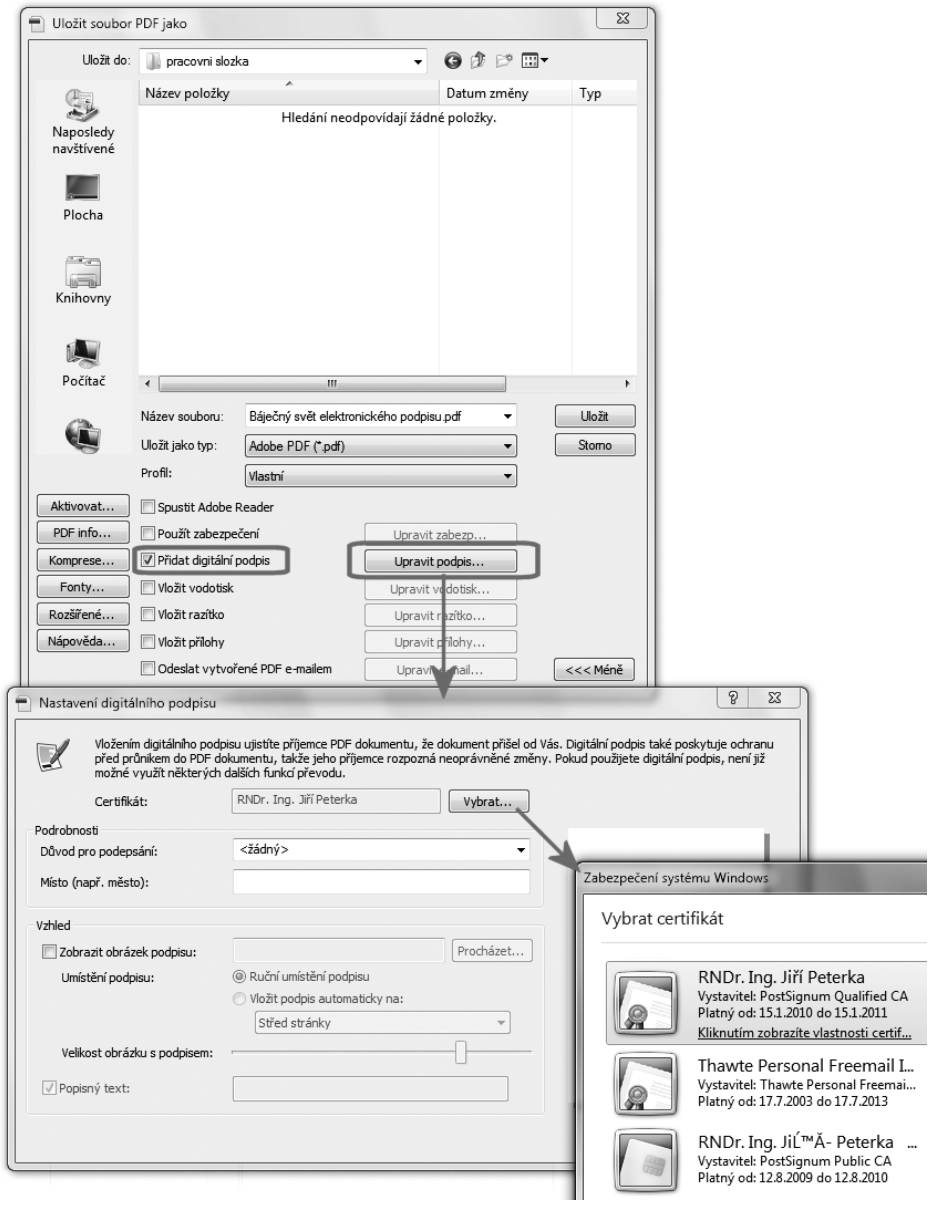


Pokud takováto virtuální PDF tiskárna podporuje i elektronické podepisování dokumentů, je třeba jí sdělit, na kterém (osobním) certifikátu má být podpis založen. Výběr certifikátu lze obvykle provést dopředu během nastavování virtuální tiskárny.

Velmi často ale lze příslušnou volbu při samotném tisku ještě změnit, pokud si uživatel přeje podepsat PDF dokument „jinak“ (založit podpis na jiném certifikátu), než jak je nastaveno na tiskárně. Příklad, ukazující použití virtuální tiskárny programu Print2PDF (od společnosti Software602), ilustruje následující obrázek.

Obrázek 6-46

Příklad podepisování PDF dokumentu, který vytváří virtuální PDF tiskárna



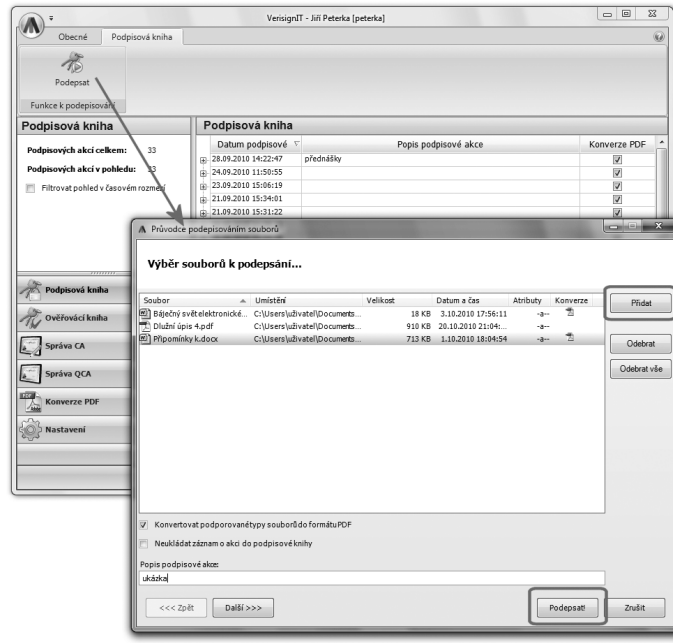
6.8.2 Samostatné konverzní programy

Programy, které slouží ke konverzi do PDF formátu, samozřejmě nemusí nutně mít jen podobu virtuální tiskárny. Stejně tak mohou fungovat i jako klasické aplikační programy: uživatel jim zadá vstupní soubor ve zdrojovém formátu (například textový dokument ve formátu editoru MS Word, s příponou .doc či .docx), a program podle něj vytvoří PDF dokument, který ihned opatří požadovaným elektronickým podpisem.

> Někdy takovéto programy nabízí obě varianty svého fungování: jak virtuální PDF tiskárnu, tak klasický program.

Příklad si můžeme ukázat na již zmiňovaném programu VerisignIT, který se dokonce snaží vytvářet iluzi „podpisové knihy“: do ní uživatel vloží jeden či více souborů a pak je nechá podepsat všechny najednou. Pokud se jedná o soubory v jiném formátu, jsou konvertovány do PDF. Stejně tak ale mohou být do „podpisové knihy“ vloženy i PDF dokumenty, které jsou pouze podepisovány.

Obrázek 6-47
Příklad výběru souborů ke konverzi a podepsání



K podpisu přitom mohou být zadány i již podepsané PDF soubory – a v takovém případě dochází k připojení dalšího podpisu k již podepsanému dokumentu. Tedy k vícenásobnému podpisu (nikoli ale souběžně, v rámci jednoho kroku, nýbrž postupně).

6.8.3 Samostatné programy pro podepisování

Vedle programů, které podepisují PDF dokumenty v okamžiku jejich vzniku (v rámci konverze), pochopitelně existují i takové, které neslouží ke konverzi, ale jen k podepisování (již existujících) PDF dokumentů. Jejich schopnosti a způsoby ovládání se mohou lišit – mohou to být velmi jednoduché programy se strohým uživatelským rozhraním, ale stejně tak to mohou být programy s větším rozsahem funkcí a komfortním způsobem ovládání.

Případně může jít o funkčnost, zabudovanou do programů, které mají primárně jiný účel. Například u různých spisových služeb, které slouží potřebám nakládání s PDF dokumenty.

Jako příklad si můžeme ukázat dva programy české provenience. Prvním je komerční program PDF Signer od společnosti Dignita. Jeho ovládání je maximálně zjednodušeno a redukuje se na přetažení souboru s PDF dokumentem na tento program. Ten to pochopí jako pokyn k podepsání podle toho jak je aktuálního nastavení – s tím, že podepsaný soubor je uložen do stejného místa jako podepisovaný soubor. Příklad vzhledu programu ukazuje následující obrázek.

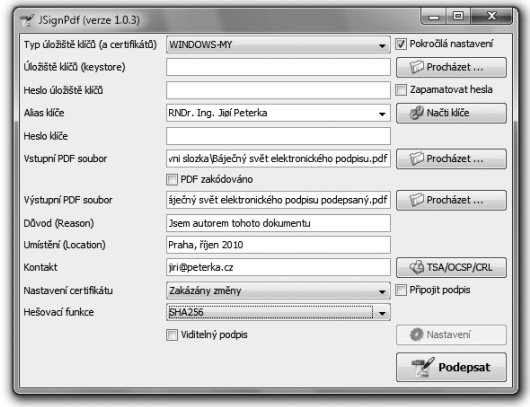
Obrázek 6-48

Program PDF Signer od spol. Dignita

Nastavení programu PDF Signer umožňuje volbu certifikátu, na kterém má být podpis založen (včetně hodnocení toho, zda je certifikát pro tento účel vůbec použitelný). Nabízeny jsou osobní certifikáty ze systémového úložiště MS Windows (ke kterým je k dispozici soukromý klíč). Standardně jsou vytvářeny pouze neviditelné elektronické podpisy na PDF dokumentech, ale program „umí“ i podpisy viditelné. Lze zadat i důvod podpisu a umístění.

Druhým příkladem je javovská aplikace JSignPDF, která je softwarem s otevřeným kódem (open-source) a může se legálně a zdarma používat jak v soukromé, tak i v komerční sféře. Tato aplikace již nabízí klasičtější rozhraní s možností explicitního výběru zdrojového i cílového souboru. Zajímavostí je možnost volby úložiště důvěryhodných certifikátů. Podporován je také viditelný podpis, stejně jako možnost zadat důvod podpisu, umístění či kontakt na podepsanou osobu.

Obrázek 6-49
Uživatelské rozhraní javovské aplikace JsignPDF

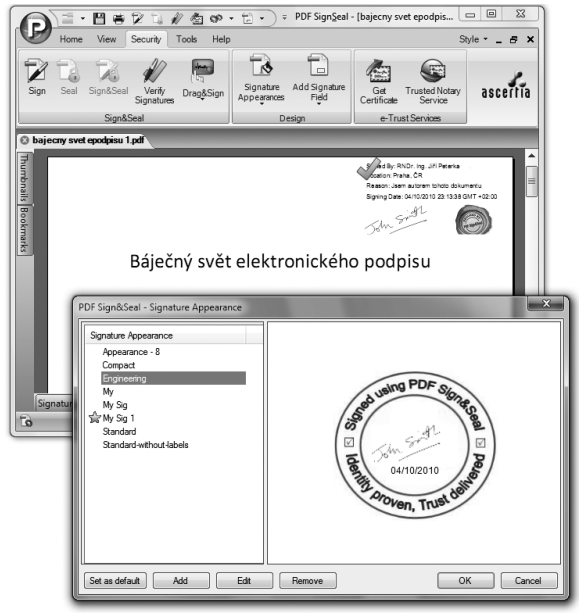


6.8.4 Vytváření viditelných podpisů

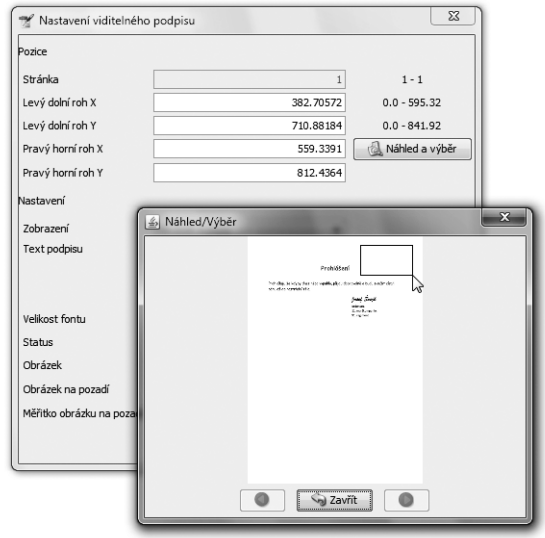
Až dosud jsme mlčky předpokládali, že vytváříme neviditelné podpisy na PDF dokumentech (viz část 6.1). Pokud bychom chtěli vytvářet podpisy viditelné, musíme pochopitelně využít takový program, který tuto možnost podporuje.

Programy, podporující viditelné podpisy, opět mohou mít různý princip fungování a odlišný uživatelský komfort. Jednou z možností je nabídka určitého repertoáru předdefinovaných viditelných podpisů s možností jejich eventuální úpravy či přidání vlastních vzhledů. Jako u programu na následujícím obrázku.

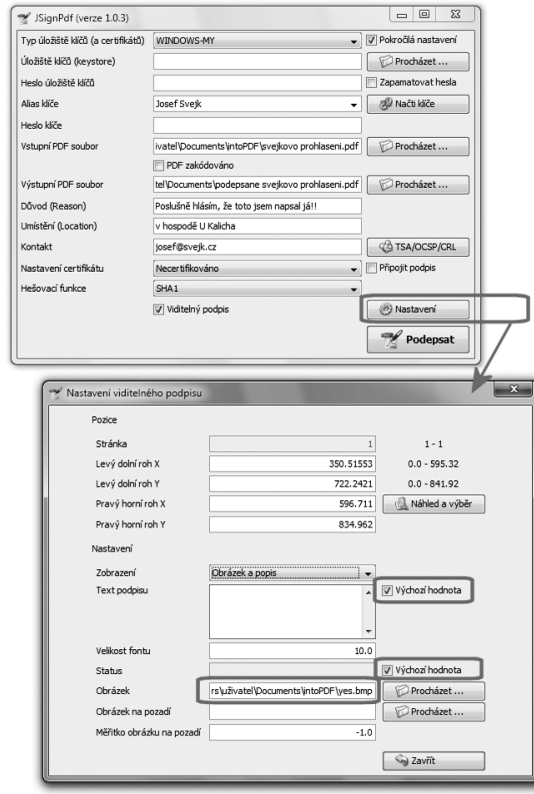
Obrázek 6-50
Příklad nabídky viditelných podpisů



Obrázek 6-51
Příklad volby umístění viditelného podpisu



Obrázek 6-52
Příklad nastavení viditelného podpisu



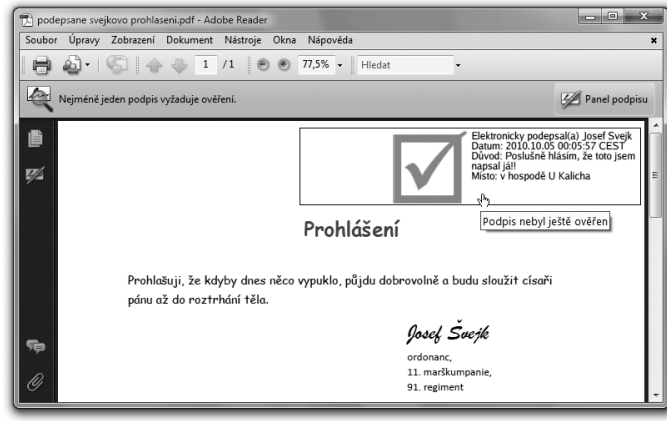
Častěji ale bývá možnost viditelných podpisů redukována jen na jednu variantu, kterou si uživatel může v jisté míře pozměnit podle svého uvážení. Zejména výběrem údajů, které mají být ve viditelném podpise obsaženy, či volbou obrázku na pozadí a na popředí – a snad vždy také umístěním samotného viditelného podpisu. Zde jsou obvykle „předdefinovány“ možnosti jako „vpravo nahoře“, „vlevo nahoře“ atd., a jen někdy má uživatel možnost volit ještě jiné umístění.

Princip „uzpůsobení“ viditelného podpisu si můžeme ukázat na příkladu již zmiňované javovské aplikace JSignPDF. Ta nabízí jednoduchou a názornou možnost umístění (volby polohy) viditelného podpisu na tištěné stránce pouhým přetažením oblasti pro podpis.

Dalším krokem pak je specifikace toho, co má viditelný podpis obsahovat. Lze zvolit jak obrázek na pozadí (zde nepoužito), tak i obrázek na popředí, a dále samotné texty. Tyto texty lze zadat buďto explicitně, nebo nechat na „výchozích“ hodnotách, tak jak jsou zadány již pro neviditelný podpis.

Příklad pro program JSignPDF vidíte na obrázcích na předchozí stránce. Výsledek, a to v podobě samotného viditelného podpisu, ukazuje následující obrázek (s podpisem literární postavy Josefa Švejka).

Obrázek 6-53
Výsledný viditelný podpis

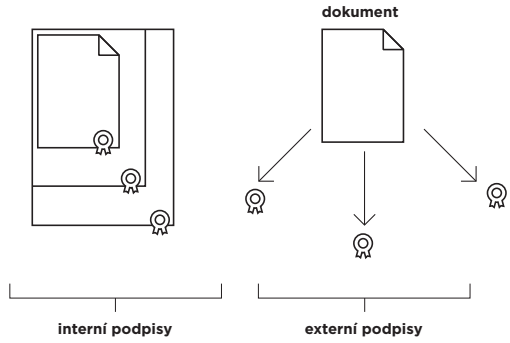


6.8.5 Vytváření externích podpisů

V souvislosti s externími elektronickými podpisy si nejprve znovu připomeňme, že jimi lze podepsat skutečně cokoli, co má podobu souboru.

Na rozdíl od interních elektronických podpisů zde totiž není požadavek na to, aby formát podepisovaného souboru podporoval interní podpisy, neboli umožňoval vkládat je „dovnitř souboru. Externí podpis je totiž zcela samostatným prvkem, který je vkládán do zcela samostatného souboru (podrobněji viz část 2.8) se specifickým formátem (a příponou), viz část 5.3.3.

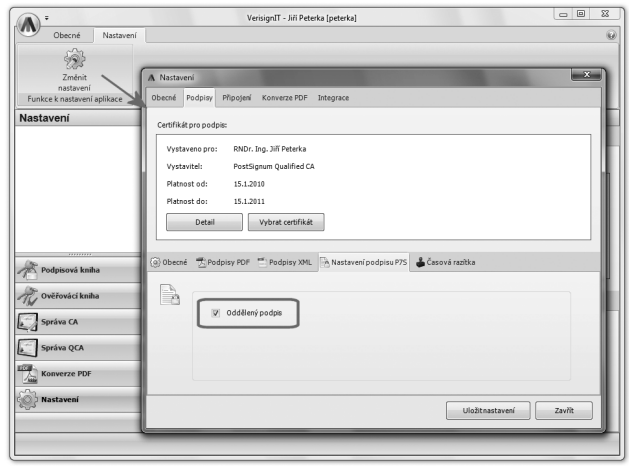
Obrázek 6-54
Představa interních a externích el. podpisů



Z této zásadní odlišnosti (oproti interním podpisům) pak plyne i zajímavá „procedurální“ odlišnost, týkající se vícenásobného podepisování: v případě, kdy má jeden a tentýž dokument podepsat více osob, je pořadí vytváření jednotlivých podpisů irelevantní. Každý jednotlivý podpis totiž vzniká jakoby „na zelené louce“ a nezávisle na tom, zda již existuje nějaký jiný externí podpis téhož dokumentu.

V případě interních podpisů tomu může být jinak. Zde již pořadí může být relevantní v závislosti na tom, jak konkrétně jsou jednotlivé interní podpisy řešeny a vkládány do podepisovaného souboru – zda každý nový podpis jakoby „obaluje“ (a současně podepisuje) celý dokument včetně jeho dosavadních podpisů, nebo zda každý podpis „pokrývá“ jen samotný obsah dokumentu bez již přidaných podpisů. Záleží tedy na konkrétním formátu a na tom, jak konkrétně podporuje interní podpisy.[11]

Obrázek 6-55
Příklad nastavení programu tak, aby vytvářel externí podpisy



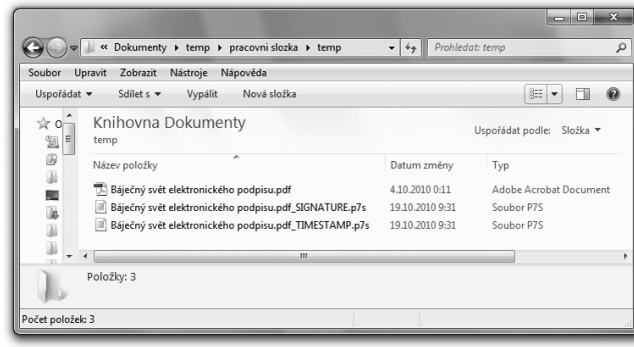
[11] Konkrétně u formátu PDF jsou interní podpisy skutečně řetězeny, v tom smyslu že každý další „pokrývá“ i předchozí podpis a skrze něj i všechny předchozí podpisy. Proto se o interních podpisech na PDF dokumentech hovoří také jako o **sériových podpisech**. Naproti tomu externí podpisy jsou obvykle **paralelními podpisy**.

Nicméně zpět k externím podpisům: k jejich vytváření pochopitelně potřebujeme takový nástroj (program), který s nimi umí pracovat. Což není zdaleka každý program, schopný vytvářet (interní) elektronické podpisy.

Další nástrahou může být správné nastavení tohoto programu tak, aby skutečně vytvářel externí podpisy místo interních. To může být komplikováno i tím, že takový program může externí podpisy nazývat jinými jmény. Například program VerisignIT od společnosti Dignita, který vidíte na následujícím obrázku, je označuje jako „oddělené“ podpisy.[12]

Dalším úkonem ze strany uživatele je určení toho, do jakého souboru má být uložen výsledný externí podpis. Ne každý program vytvářející externí podpisy ale toto vyžaduje či jen umožňuje. Některé si jméno a příponu souboru pro externí podpis (a třeba i časové razítko) vytváří samy, určitým systematickým odvozením ze jména podepisovaného souboru. Příklad (pro zde použitý program VerisignIT) vidíte na následujícím obrázku. Povšimněte si na něm ještě jedné zajímavosti: data vzniku, resp. poslední změny souboru.

Obrázek 6-56
Příklad externího podpisu (a externího časového razítka) k podepsanému PDF dokumentu



V případě interního podpisu by datum (poslední změny) podepsaného souboru mělo odpovídat okamžiku vzniku podpisu.[13] Naproti tomu u externího podpisu se samotný podepisovaný soubor nemění, a jeho datum proto zůstává beze změny. Na aktuální datum a čas (v okamžiku podpisu) je nastaven pouze soubor s externím podpisem (a zde konkrétně i soubor s externím časovým razítkem).

Zdůrazněme si ale, že i zde jde o negarantované časové údaje, převzaté z aktuálního nastavení systémových hodin počítače.

Jinak samotné vytvoření externího podpisu, po potřebném nastavení programu (tak, aby vytvářel externí podpisy) by se již nemělo lišit od postupu vytváření interních podpisů.

12 Což koresponduje s obvyklým označením externích podpisů v angličtině, kde jsou označovány jako **detached signatures**.

13 Alespoň na platformě MS Windows, které u souborů evidují pouze datum jejich poslední modifikace.

6.8.6 Přidávání (podpisových) časových razítek

Připojování časových razítek k elektronickým podpisům na PDF dokumentech může být v běžné praxi stejně jednoduché, jako samotné podepisování, resp. vytváření podpisů. Pokud totiž správně nastavíme ten program, který pro podepisování používáme, může on za nás přidávat časová razítka k vytvářeným podpisům zcela automaticky, aniž se musíme o cokoli starat.

Připomeňme si v této souvislosti, že u PDF dokumentů je interní časové razítko standardně „nesamostatné“, v tom smyslu že jej nelze přidat k dokumentu samostatně, ale vždy jen jako součást elektronického podpisu (jako garantovaný časový údaj v rámci elektronického podpisu).[14] Proto je také označováno jako „podpisové“ časové razítko.

V případě externího časového razítka tomu může být jinak, protože externí časové razítko je ukládáno do samostatného souboru (viz předchozí příklad). A tak zde záleží na tom, co umožní příslušný program: zda umožní vytvořit pouze externí časové razítko, nebo zda jej umožňuje vytvořit jen současně s (externím) elektronickým podpisem.

Nutnou podmínkou toho, aby námi používaný program mohl přidávat (podpisová) časová razítka k právě vytvářeným podpisům, je jeho správné nastavení, resp. „provázání“ s příslušnou autoritou časových razítek, která tato razítka generuje.

Připomeňme si, v souladu s částí 2.7, jak vlastně časové razítko vzniká: program, který uživatel používá, vygeneruje otisk podepisovaného dokumentu a odešle jej příslušnému poskytovateli (autoritě časového razítka). Ten na základě otisku vygeneruje časové razítko, které vrátí zpět, a program jej připojí k dokumentu.

Aby tento scénář mohl fungovat, musí mezi uživatelem a příslušným poskytovatelem časových razítek existovat dohoda o poskytování služby. Alespoň v případě kvalifikovaných časových razítek jde typicky o placenou službu a poskytovatel musí vědět, komu službu poskytuje a kam má poslat účet.[15]

Další nezbytnou podmínkou je pak schopnost používaného programu „domluvit se“ s autoritou časových razítek takovým způsobem, aby obě strany mohly vzájemně komunikovat a předávat si v jednom směru otisky dokumentů, a ve druhém směru samotná časová razítka.[16] Včetně toho, aby autorita časových razítek měla jistotu, že jde skutečně o jejího zákazníka a ne o někoho jiného, kdo by se za něj jen vydával (a na jeho účet si nechával vystavovat časová razítka).

---

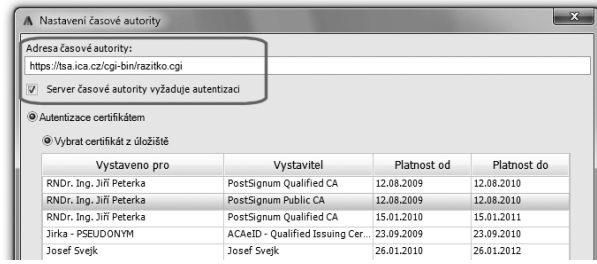
14 S výjimkou archivních časových razítek, viz část 6.11.

15 Toto samozřejmě nevylučuje existenci takových poskytovatelů kvalifikovaných časových razítek, kteří by své služby poskytovali zdarma. V případě časových razítek pro testovací účely (tj. nikoli kvalifikovaných časových razítek) je jejich poskytování zdarma naopak zcela obvyklé.

16 Toto je definováno v RFC 3161.

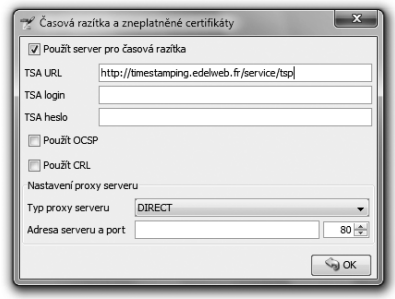
Identifikace a autentizace zákazníka v roli žadatele o časové razítko může vyžadovat (komerční) certifikát (jako například u I. CA), nebo může být založena jen na správném zadání uživatelského jména a hesla. Příklad nastavení, pro program VerisignIT vidíte na následujícím obrázku:

Obrázek 6-57
Příklad nastavení autority časového razítka



V případě časových razítek, generovaných pro potřeby testování, nemusí být identifikace a autentizace žádná a časové razítko je poskytnuto komukoli, kdo si o něj „řekne“. I v tomto případě je ale nutné zadat správný URL odkaz na příslušného poskytovatele služby časových razítek tak, aby program žádající o razítko věděl, kam příslušnou žádost poslat. Příklad pro službu poskytující testovací časová razítka vidíte na obrázku, pro program JSignPDF. Ten ale nenabízí možnost autentizace prostřednictvím certifikátu (jako VerisignIT na předchozím obrázku), ale jen pomocí jména a hesla (pokud je požadováno).

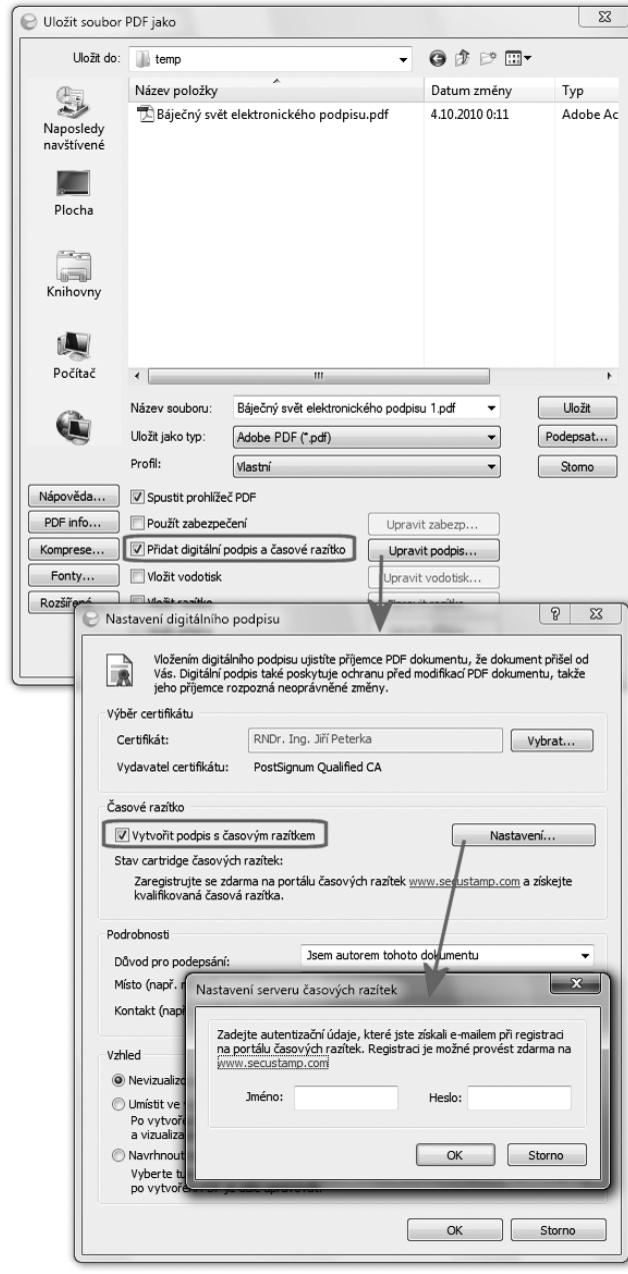
Obrázek 6-58
Příklad nastavení autority časového razítka v programu JSignPDF



Jiným příkladem může být verze 9 programu Print2PDF od společnosti Software602. Ta již také podporuje přidávání časových razítek a zajímavým způsobem řeší i ekonomickou stránku věci: nenutí uživatele, aby si sám sjednával smlouvu s autoritou časových razíte, a té pak také platil za skutečně využitá časová razítka.

Místo toho je zde využit princip předplatného: uživatel si dopředu zakoupí určitý „balíček“ kvalifikovaných časových razítek, které pak využívá (čerpá).

Obrázek 6-59
Příklad práce s časovými razítky v programu Print2PDF



Navíc toto předplatné uživatel nesjednává přímo s autoritou časových razítek (kterou je zde I. CA), ani s ní neuzavírá jakoukoli smlouvu.

Místo toho si „balíčky“ časových razítek kupuje od producenta programu (Software602), přes specializovaný portál SecuStamp, provozovaný na adrese *http://secustamp.com*.

Veškeré potřebné nastavení nutné k práci s časovými razítky je již zabudováno do programu Print2PDF. Jediné, co uživatel musí doplnit, je jméno a heslo k jeho „balíčku“, které získá při registraci na portálu a nákupu balíčku, viz přechozí obrázek.

6.9 Podepisování PDF dokumentů programem Adobe Acrobat

Pro práci s PDF dokumenty lze samozřejmě lze použít i nástroje (programy) přímo od společnosti Adobe, která formát PDF vyvinula. Z celé plejády těchto nástrojů se podrobněji zastavíme u dvou různých produktů, které reprezentují dva odlišné přístupy k podepisování: u programu Adobe Acrobat, který je placeným (komerčním) programem a u Adobe Readeru, který je k dispozici zdarma. Přesto i on nabízí určité možnosti podepisování elektronických dokumentů ve formátu PDF.

Nejvíce možností pro vytváření elektronických podpisů pochopitelně poskytuje „vlajková loď“ Adobe pro PDF dokumenty, kterou je program Adobe Acrobat. Ten umožňuje vytvářet a přidávat k PDF dokumentům snad všechny možné varianty interních elektronických podpisů – certifikační podpisy i podpisy „běžné“, podpisy viditelné i neviditelné, s časovými razítky i bez nich. Stejně tak umožňuje přidávat více podpisů na jeden a tentýž dokument.

Adobe Acrobat navíc dokáže „připravit“ PDF dokument (tzv. odemknout ho, resp. aktivovat) tak, aby mohl být následně podepsán ve volně šiřitelném programu Adobe Reader.

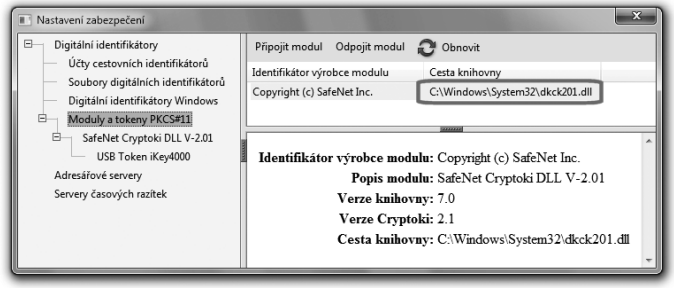
Co ale Adobe Acrobat neumí, je vytvářet externí podpisy. Specializuje se jen na podpisy interní.

6.9.1 Nastavení programu Adobe Acrobat

I program Adobe Acrobat pochopitelně vyžaduje určité nastavení. Pro potřeby vyhodnocování elektronických podpisů je toto nastavení v zásadě stejné, jako u programu Adobe Reader, které jsme si popisovali v části 6.5. Tedy včetně toho, zda má využívat „integraci s MS Windows“.

Jinými slovy: i Adobe Acrobat, stejně jako Adobe Reader, pracuje buďto s vlastním úložištěm certifikátů, nebo (v případě „integrace“) jej rozšiřuje i o systémové úložiště MS Windows. V obou případech se obsah úložiště bude využívat jak pro potřeby vyhodnocování platnosti podpisů (ohledně důvěryhodnosti certifikátů), tak i pro potřeby vytváření podpisů: Acrobat nabídne možnost založit podpis na takovém certifikátu, který najde v aktuálně dostupném úložišti a ke kterému je k dispozici soukromý klíč.

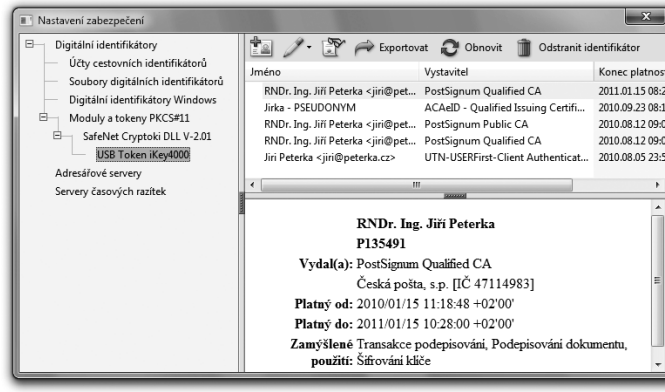
Obrázek 6-60
Příklad zpřístupnění externího úložiště, přes systémovou knihovnu



Acrobat dokáže pracovat i s různými externími (vyjímatelnými) úložišti, typu USB tokenů či čipových karet. Ty se mu ale musí nejprve správně zpřístupnit, způsobem, který jsme v obecné rovině popsali v části 5.1.3. Připomeňme si, že hlavním požadavkem je sdělit příslušnému programu (zde tedy Adobe Acrobatu), skrze kterou systémovou knihovnu má příslušné úložiště ovládat. Pak již si dokáže sám zpřístupnit obsah příslušného úložiště a pracovat s ním tak, jak naznačují obrázky.

Adobe Acrobat (a stejně tak i Reader, viz dále) dokáže pracovat ještě s dalším typem externího úložiště, kterým je jakési „roamingové“ úložiště. Tedy jedno centrální místo (resp. centrální server), kde má uživatel bezpečným způsobem uloženy své certifikáty i odpovídající soukromé klíče – a správně nastavený program Acrobat s nimi dokáže pracovat. Jde o certifikáty a klíče, které česká lokalizace produktů Adobe označuje jako „cestovní identifikátory“ (zatímco anglická verze hovoří o „roamingových identifikátorech“).

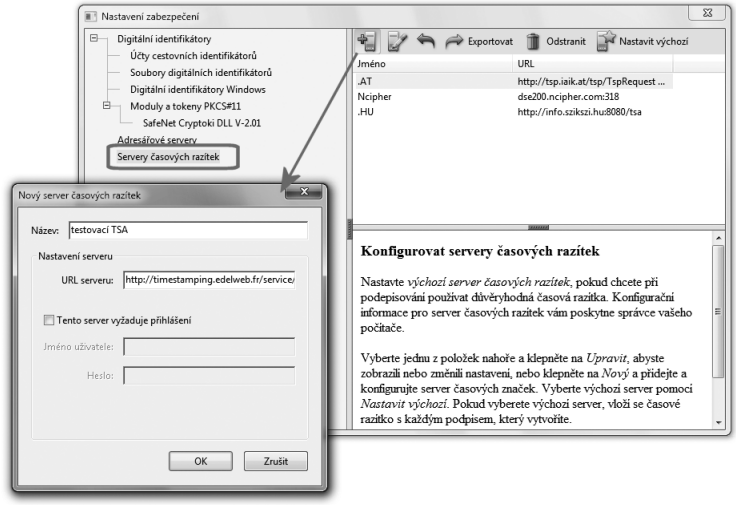
Obrázek 6-61
Příklad obsahu externího úložiště, který je k dispozici programům Adobe Acrobat i Reader



Ještě další nastavení programu Acrobat je nutné v tom případě, kdy uživatel chce připojovat ke svým podpisům také časová razítka. Zde je nutné programu Acrobat sdělit, „odkud“ je má získávat.

Princip práce s časovými razítky je principiálně stejný jako v případě programů třetích stran, tak jak jsme si jej popisovali v části 6.8.6. Adobe Acrobat (ve verzi dostupné v době vzniku této knihy) ale bohužel nenabízí možnost autentizace uživatele pomocí certifikátu – ale jen pomocí jména a hesla.

Obrázek 6-62
Příklad nastavení autority časového razítka



Postup nastavení autority časového razítka ukazuje předchozí obrázek. Uživatel si takovýchto nastavení (různých poskytovatelů, resp. autorit časového razítka) může vytvořit více, a jedno z nich by měl prohlásit za výchozí.[17] Podle něj (resp. od příslušné autority) je pak časové razítko automaticky přidáváno ke každému jednotlivému elektronickému podpisu (bez dalších dotazů, tedy i bez možnosti volby jiného zdroje časového razítka).

6.9.2 Náhled podpisu

Při podepisování PDF dokumentů, ať již jakýmikoli prostředky, musíme pamatovat na to, že tyto dokumenty nemusí obsahovat jen to, co právě vidíme na obrazovce, když se na ně díváme skrze Adobe Reader či Adobe Acrobat, případně jiným programem. Formát PDF má totiž celou řadu možností, díky kterým může obsahovat i takový obsah, který nemusí být v aktuálním režimu zobrazení právě patrný.

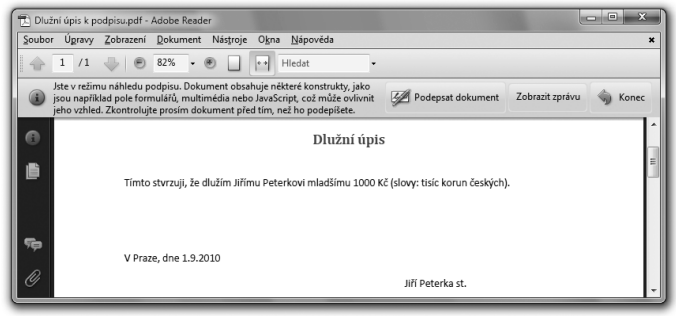
Nejjednodušším příkladem mohou být různé poznámky v textu, složitějším pak například různé skripty, a nejzáludnější je asi možnost udělat z PDF dokumentu rovnou celý kontejner, do kterého je možné vkládat v zásadě jakékoli soubory. Jenže při podepisování se fakticky podepisuje vše, co PDF dokument právě obsahuje – a co nemusí být zrovna vidět.

Aby uživatel nepodepisoval něco, o čem neví, je Adobe Acrobat (ale i Reader) vybaven režimem náhledu podpisu, při kterém upozorňuje na to, zda je v dokumentu právě nějaký obsah, který není zobrazen, nebo který by mohl měnit obsah souboru. Je pak na uživateli, zda využije tuto možnost a seznámí se s tím, co všechno PDF dokument obsahuje. Ze zákona (č. 227/2000 Sb., o elektronickém podpisu) ale platí presumpce toho, že se se vším seznámil.

[17] Pokud tak neučiní, nejsou k vytvářeným podpisům časová razítka přidávána vůbec.

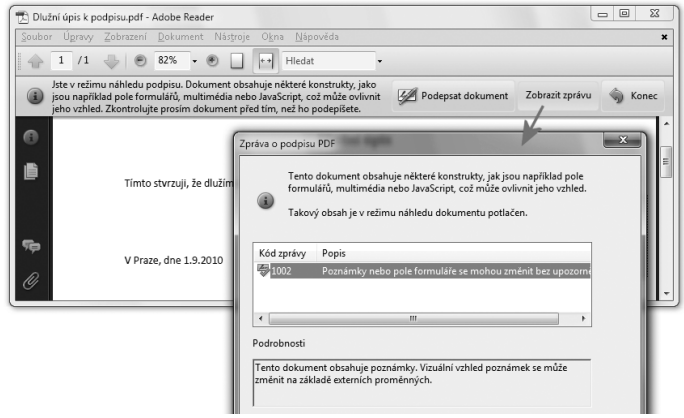
Příklad upozornění na nezobrazený či aktivní obsah (v režimu náhledu podpisu) ukazuje následující obrázek. Z něj je patrné pouze to, že nějaký takový obsah v dokumentu obsažen je, ale ještě neříká, o co konkrétně jde.

Obrázek 6-63
Příklad dokumentu, u kterého režim náhledu podpisu indikuje aktivní či nezobrazený obsah



Konkrétnější informaci o tom, o jaký obsah jde, lze získat z nabídky „Zobrazit zprávu“.

Obrázek 6-64
Příklad informace o nezobrazeném či aktivním obsahu v PDF dokumentu

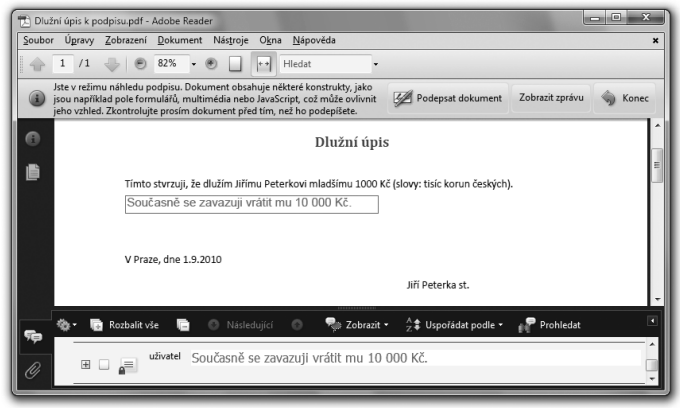


Ve zde použitém příkladu se konkrétně jednalo o skryté poznámky, resp. komentáře – a které po svém zobrazení zásadně mění smysl celého PDF dokumentu.

Pamatujme tedy na to, abychom se před podepsáním PDF dokumentu vždy seznámili s veškerým jeho obsahem, který se chystáme podepsat, včetně všech „skrytých“ částí a prvků. Adobe Acrobat (stejně jako Reader) nám v tom ohledu vychází vstříc dvěma různými cestami.

Obrázek 6-65

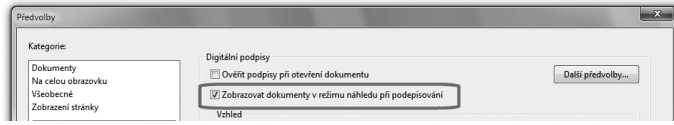
PDF dokument se zobrazenými komentáři



První cestou je samotné zapnutí režimu náhledu při podepisování. To lze zvolit v nastavení předvoleb, v části věnované zabezpečení, viz obrázek:

Obrázek 6-66

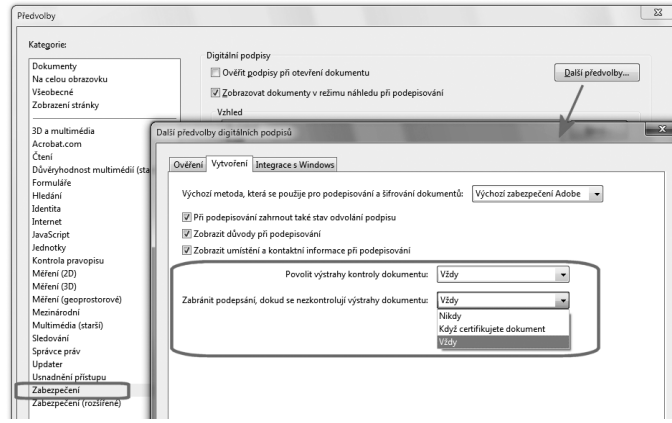
Zapnutí režimu náhledu při podepisování



Druhá cesta vede přes nastavení toho, aby se seznámení se zprávami (výstrahami) o skrytém či aktivním obsahu stalo povinné a bez něj nebylo možné dokument podepsat. Opět se volí v rámci předvoleb (přes Další předvolby a zde záložka „Vytvoření“).

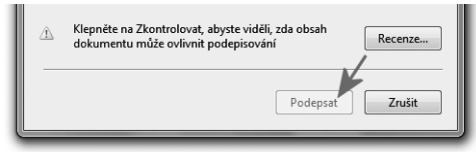
Obrázek 6-67

Nastavení povinné kontroly výstrah dokumentu



Pokud je tato druhá možnost navolena (aktivní), pak při samotném podepisování není možnost podpisu aktivní, dokud uživatel nepotvrdí, že se seznámil se zprávami o skrytém či aktivním obsahu v PDF dokumentu.

Obrázek 6-68
Dokud se uživatel neseznámí s obsahem, nemůže skutečně podepsat



6.9.3 Druhy podpisů

Než se pustíme do toho, jakým způsobem fungují jednotlivé možnosti podepisování dokumentů v programu Adobe Acrobat, udělejme si nejprve malý přehled, resp. shrnutí těchto možností. Některé z nich si totiž zaslouží určité vysvětlení.

V prvním přiblížení lze konstatovat, že Adobe Acrobat nabízí čtyři varianty elektronických podpisů:

- certifikační podpis
- „schvalující“ podpis
- prázdný podpis
- „ruční“ podpis

S první variantou jsme se již seznámili v části 6.2: **certifikační podpis** jakoby „schvaluje formulář“, který je následně možné vyplňovat. Jde tedy o takový podpis, u kterého je možné (ale nikoli nutné) povolit určité následné změny. Například právě vyplňování položek formuláře, nebo další podepisování. Adobe Acrobat přitom nabízí certifikační podpisy jak ve viditelném provedení (s určitou „vizuální podobou“ na samotném dokumentu, tak i v neviditelném provedení, kdy na samotném dokumentu (ani po jeho tisku) není patrné, že je elektronicky podepsán.

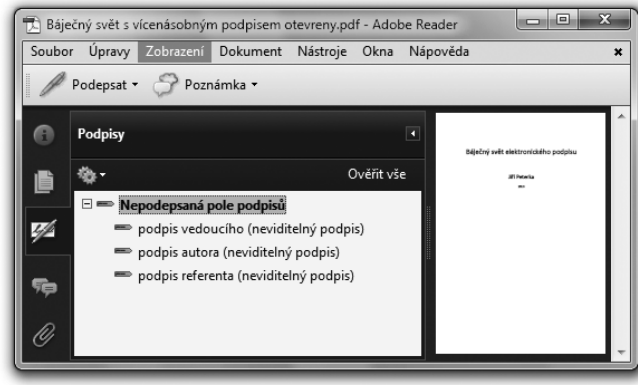
Druhou variantou je **„schvalující“ podpis** (anglicky **approval signature**). Jde o ten druh elektronického podpisu, o kterém primárně pojednává celá tato kniha a který vyjadřuje určitou formu schválení, resp. souhlasu (ve smyslu zákona a jeho konstatování, že „dokument podepsala osoba ….“). Byť neformálně (a bez opory v zákoně) je důvod podpisu možné detailněji popsat, například formulacemi jako „Jsem autorem tohoto dokumentu“, „Schvaluji tento dokument“ a podobně (viz část 6.4).

Adobe Acrobat nabízí tyto „schvalující“ podpisy jako viditelné, i jako neviditelné. Primárně je ale vytváří pouze jako viditelné. Pokud uživatel potřebuje vytvořit přímo v Acrobatu podpis neviditelný, možné to je, ale musí se to udělat nepřímo, přes „prázdný“ podpis.

Prázdný podpis si můžeme představit jako druh formulářového pole, které je určeno k tomu, aby se do něj někdy později vložil elektronický podpis. A ten již může být jak viditelný, tak i neviditelný. Přesněji: jako viditelný či neviditelný se vytváří již samotný prázdný podpis, a to pak určuje viditelnost následně vloženého podpisu. Přitom „vkládání" elektronického podpisu do prázdného pole pro podpis je možné jak v programu Adobe Acrobat, tak i v programu Adobe Reader.

Příklad PDF dokumentu s připravenými prázdnými podpisy ukazuje následující obrázek. Z něj je patrné i to, že každý prázdný podpis může být popsán tak, aby to usnadňovalo jeho využití (aby bylo zřejmé, pro podpis které osoby je konkrétní formulářové pole určeno.

Obrázek 6-69
Příklad PDF dokumentu s dosud nevyplněnými prázdnými podpisy



Konečně poslední možností je **„ruční" podpis** (v angličtině **Ink Signature**, doslova inkoustový podpis). Spočívá v možnosti nakreslit do PDF dokumentu libovolnou křivku či skupiny křivek, které mohou (ale nemusí) odpovídat křivkám, které člověk vytváří při vlastnoručním podpisu. Smysl to má zřejmě jen tam, kde je možné použít vstup přes dotykovou obrazovku (tj. „podepsat se" přímo na displej, například u tabletu). A s elektronickým podpisem (v právním slova smyslu) to nemá nic společného.

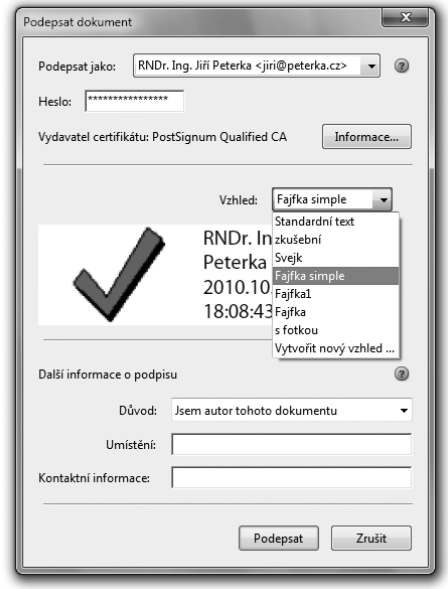
Obrázek 6-70
Představa ručního podpisu na PDF dokumentu

6.9.4 Správa viditelných podpisů

Program Adobe Acrobat je výrazně orientován na tvorbu viditelných podpisů, a tak nabízí možnost připravit si několik vzhledů těchto podpisů, a pak je podle vlastní volby uživatele aplikovat.

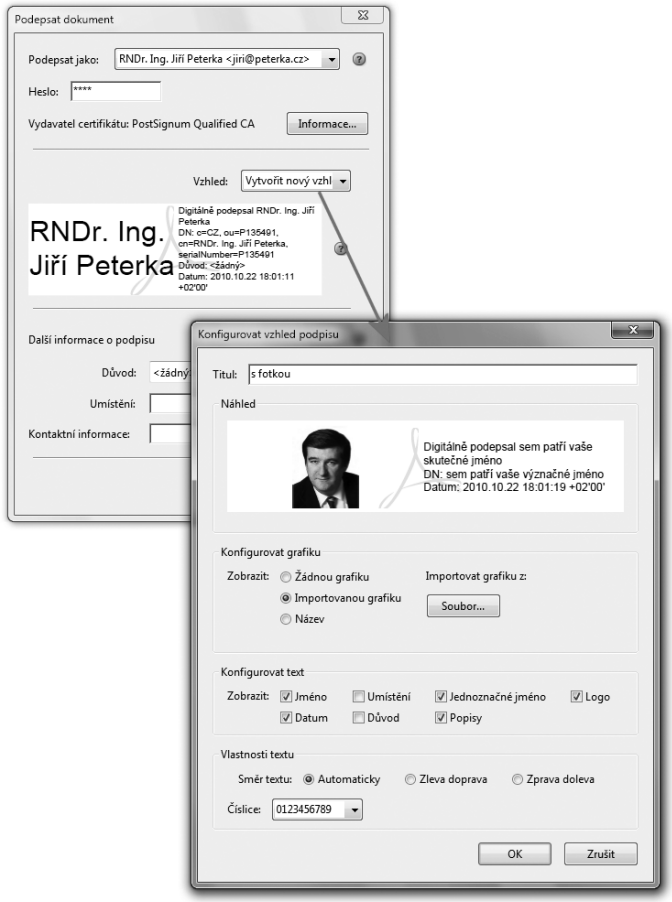
Možnost vytvořit si vlastní vzhled podpisu vede přes volbu „Vytvořit nový vzhled …“ ve výčtu již existujících vzhledů. Následně se uživateli nabídne možnost vytvořit si vlastní vzhled, na kterém může měnit jak obrázek (který může být skutečně čímkoli, například fotografií, snímkem vlastnoručního podpisu, symbolem apod.). Může to ale být jen jeden obrázek, a nikoli více obrázků zobrazovaných variantně podle toho, zda je podpis ověřen či nikoli. Obrázek ale může i chybět, a místo něj se pak zobrazuje jméno podepisující osoby, převzaté z certifikátu.

Obrázek 6-71
Výběr vzhledu viditelného podpisu

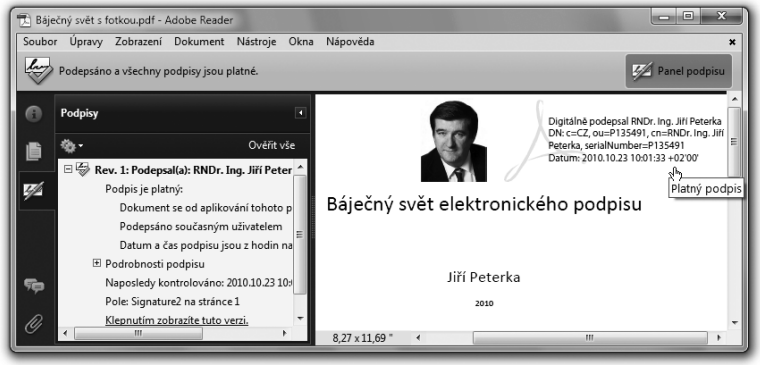


Dále je možné přidávat do volitelného podpisu další údaje, převzaté z certifikátu (jako je celé „jednoznačné jméno“, tj. jméno DN), dále údaje dodané podepisující osobou (umístění, důvod podpisu), či datum a čas (převzaté z hodin místního počítače či z časového razítka).

Každá položka s údaji ve viditelném podpisu také může mít vlastní popis (pokud je tato volba zaškrtnuta). Příklad viditelného podpisu, vytvořeného podle předem připraveného vzhledu, ukazuje spodní obrázek na následující stránce.



Obrázek 6-72
Příklad tvorby vlastního vzhledu viditelného podpisu



Obrázek 6-73
Příklad viditelného podpisu na PDF dokumentu

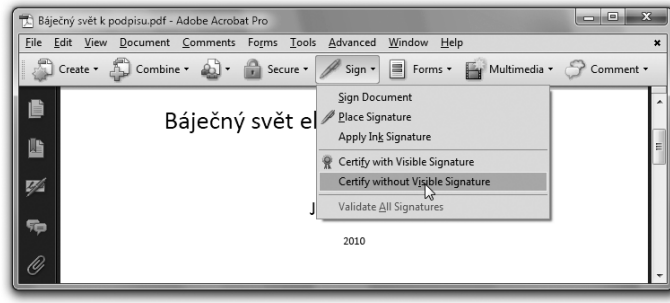
6.9.5 Certifikační podpisy

Připomeňme si, že certifikační podpisy jsou takové, které podepisují dokument, nicméně umožňují v něm následně provádět určité změny – takového charakteru a v takovém rozsahu, jak je specifikováno v okamžiku vzniku certifikačního podpisu. Smyslem je především to, aby se mohlo jednat o formulář: jeho vydavatel jej podepíše formou certifikačního podpisu, a přitom povolí vyplňování polí formuláře. Uživatel, který formulářová pole vyplní, následně může podepsat dokument svým „schvalovacím" podpisem, a to již celý, včetně vyplněných polí.

Z tohoto předpokládaného využití vychází i pravidlo o tom, že certifikační podpis musí být prvním podpisem na dokumentu. Protože pokud by nebyl, byl by „před ním" nějaký jiný („schvalující") podpis, který by „fixoval" celý dokument (včetně formulářových polí) a neumožňoval by jakoukoli změnu. Přesněji při jakékoli změně by se tento podpis stal neplatným, kvůli porušení integrity.

Příklad prvního kroku při vytváření certifikačního podpisu v programu Adobe Acrobat ukazuje následující obrázek.

Obrázek 6-74
Volba viditelného či neviditelného certifikačního podpisu

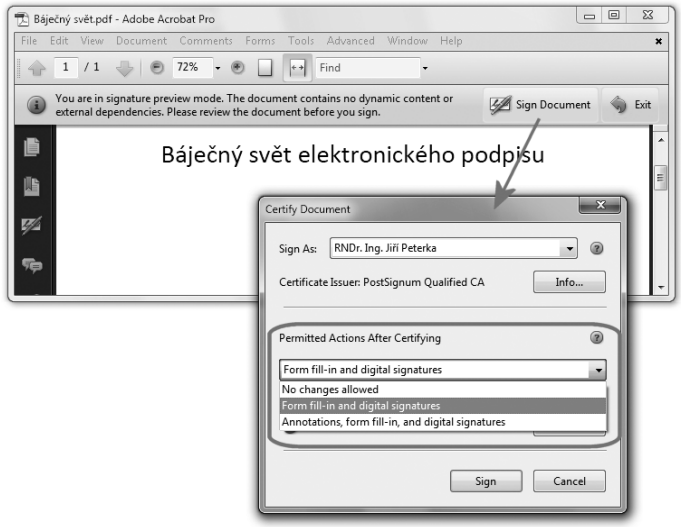


I z menu na tomto obrázku je patrné, že certifikační podpisy mohou být viditelné (visible) i neviditelné (invisible). V případě viditelného podpisu je uživatel nejprve vyzván k tomu, aby myší zvolil obdélník, do kterého bude viditelný certifikační podpis umístěn. Další postup je pak již stejný jako u podpisu neviditelného: uživatel musí vybrat certifikát, na kterém má být jeho certifikační podpis založen. Pokud je to tak nastaveno (viz část 6.9.2), musí uživatel potvrdit i to, že se seznámil se zprávami (výstrahami kontroly) o nezobrazeném či aktivním obsahu.

Především ale musí uživatel Adobe Acrobatu, který právě vytváří svůj certifikační podpis, stanovit jaké změny budou přípustné po podepsání certifikačním podpisem, aniž by tento podpis ztratil svou platnost. Možnosti jsou (viz další obrázek):

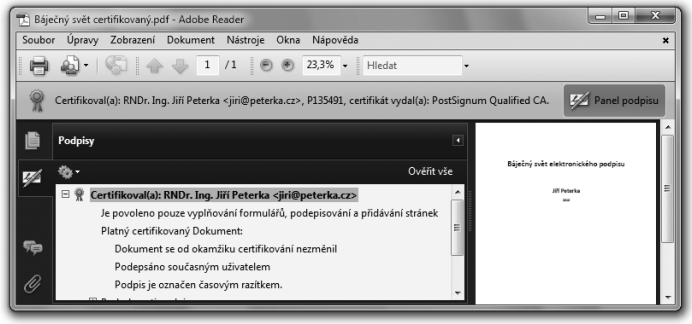
- žádné změny
- je možné vyplňování formulářů a podepisování
- jsou možné anotace, vyplňování formulářů a podepisování

Obrázek 6-75
Další postup vytváření certifikačního podpisu



Výsledkem pak může být certifikační podpis v takové podobě, jakou známe již z předchozích částí této knihy:

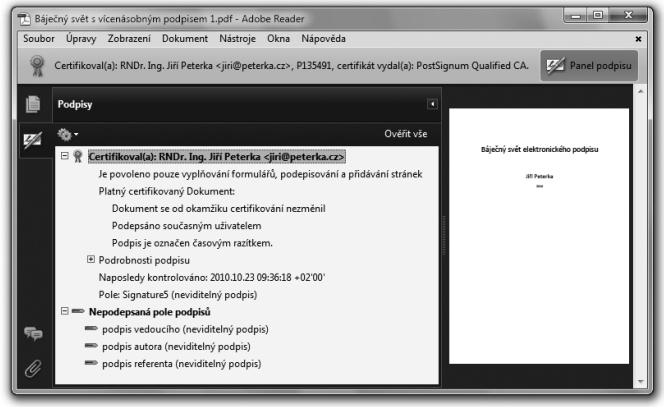
Obrázek 6-76
Příklad dokumentu, opatřeného certifikačním podpisem, s možností vyplňování formulářů a podepisování



Je-li certifikační podpis určen především pro „certifikaci“ formulářů, do kterých někdo jiný následně vyplňuje nějaké hodnoty, musí být možné takto vyplněné hodnoty také podepsat. Či spíše: podepsat, tentokráte již „schvalovacím“ podpisem, vyplněný formulář, opatřený certifikačním podpisem (který musí být na dokumentu jako první).

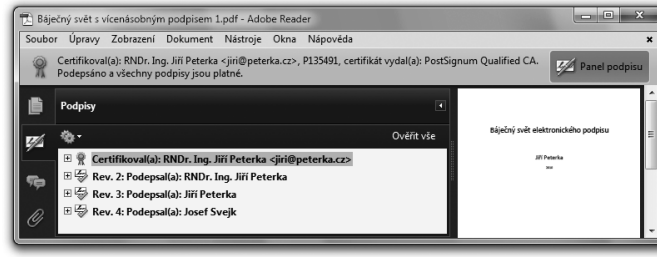
Toto je samozřejmě možné – ale s tím důležitým dodatkem, že na to musí být pamatováno ještě před připojením certifikačního podpisu, formou připojení tolika prázdných podpisů, kolik je třeba (kolik má být následných „schvalujících“ podpisů).

Obrázek 6-77
Příklad certifikovaného dokumentu s přípravou na další podpisy



Teprve pak je možné připojovat další podpisy k dokumentu, který je již opatřen certifikačním podpisem.

Obrázek 6-78
Příklad PDF dokumentu s jedním certifikačním podpisem a třemi „schvalujícími“ podpisy



Připomeňme si také to, s čím jsme se seznámili již v části 6.2: že certifikační podpisy lze považovat za zaručené elektronické podpisy (a v závislosti na certifikátu i za uznávané podpisy) do té doby, než v certifikovaném dokumentu dojde k nějaké (jakékoli) změně.

6.9.6 Prázdné podpisy

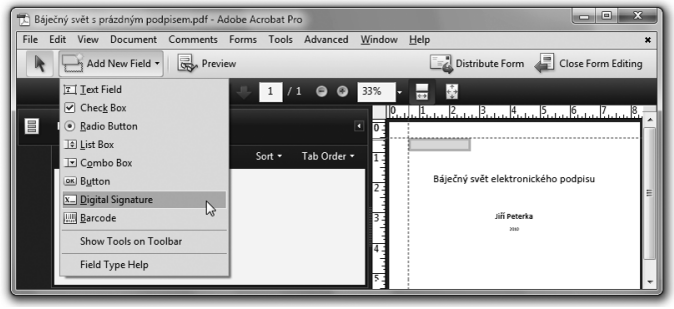
Jak jsme si již uvedli, jsou prázdné podpisy v zásadě formulářovými poli, určenými k tomu, aby se do nich (někdy později) vyplnil něčí elektronický podpis. Proto jistě nepřekvapí, že cesta k vytváření takovýchto prázdných podpisů vede přes práci s formuláři. Konkrétně přes přidání nového formulářového pole – charakteru elektronického podpisu.

Formulářové pole pro budoucí podpis je vždy třeba umístit někam do samotného dokumentu, viz první obrázek na následující stránce. Přitom je možné toto pole i pojmenovat.

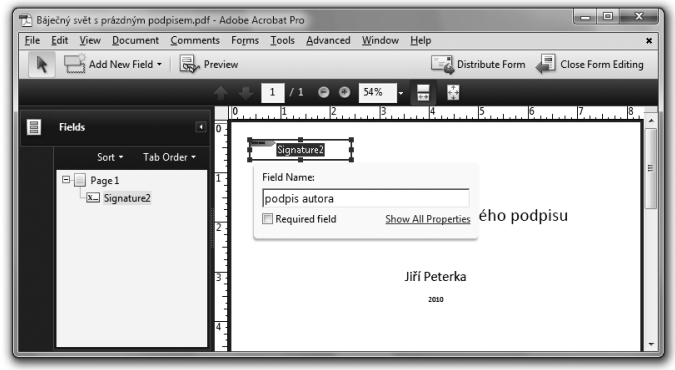
Ani (povinné) umístění nového formulářového pole do dokumentu ale stále ještě neznamená, že následně vložený podpis bude viditelný. Jak toto formulářové pole, tak i následně vložený podpis totiž stále

mohou být buď viditelnými, nebo neviditelnými – to lze zvolit skrze vlastnosti vkládaného komentářového pole (v angličtině přes nabídku Show All Properties).

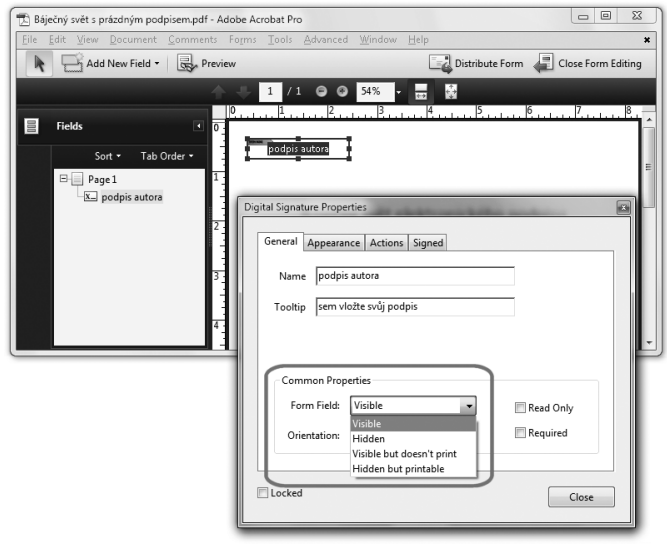
Obrázek 6-79
Přidávání formulářového pole do PDF dokumentu



Obrázek 6-80
Umístění formulářového pole pro budoucí podpis



Obrázek 6-81
Volba toho, zda pole i budoucí podpis budou viditelné či nikoli

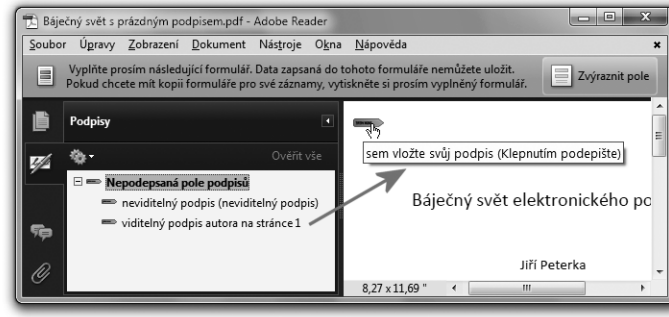


V úvahu dokonce připadají ještě dvě další možnosti, a to:

- viditelný podpis, který se ale netiskne (Visible but doesn't print)
- neviditelný podpis, který se ale tiskne (Hidden but printable)

Výsledný „vzhled" prázdných podpisů ukazuje následující obrázek. Je na něm PDF dokument se dvěma prázdnými podpisy, jedním viditelným a jedním neviditelným.

Obrázek 6-82
Vzhled PDF dokumentu s viditelným a neviditelným prázdným podpisem



6.9.7 „Schvalující" podpisy

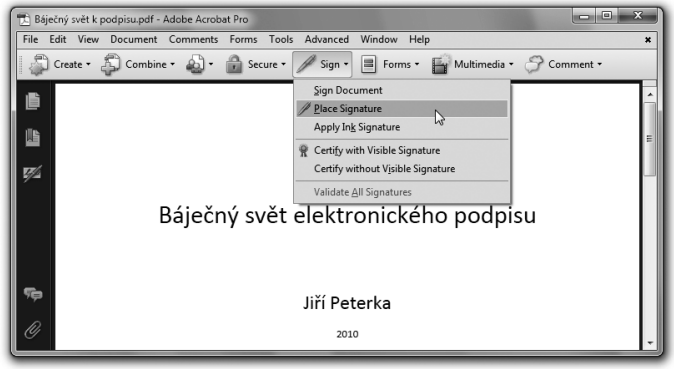
Připomeňme si, že pro podpisy a podepisování v tradičním pojetí jsou u produktů Adobe určeny elektronické podpisy, označované jako „schvalující" (approval signatures), případně jen „podpisy" (bez dalšího přívlastku) – a že tyto podpisy jsou alternativou k certifikačním podpisům. Věcný rozdíl mezi nimi je ten, že po přidání „schvalujícího" podpisu již není možné podepsaný dokument měnit (bez porušení integrity a tím i neplatnosti podpisu), zatímco po přidání certifikačního podpisu jsou určité změny možné, v rozsahu stanoveném při vzniku certifikačního podpisu.

Program Adobe Acrobat se při práci se „schvalujícími" podpisy ale chová poněkud specificky, když se uživateli snaží vnutit vždy jen viditelnou variantu takovéhoto podpisu. Máte-li „čistý" dokument, který není opatřen jiným podpisem (a to ani tím prázdným), umožní vám přidat pouze viditelný podpis. Neviditelný vám umožní přidat pouze v případě, kdy je podepisovaný dokument opatřen prázdným podpisem (který je nastaven jako neviditelný).

S tímto důležitým momentem souvisí i správná interpretace nabídek a položek menu, které Acrobat nabízí v souvislosti se „schvalujícími" podpisy:

- vytvoření neviditelného podpisu nabízí skrze položku „Podepsat dokument" (v angličtině: Sign Document)
- vytvoření viditelného podpisu nabízí skrze položku „Umístit podpis" (v angličtině Place Signature)

Obrázek 6-83
Nabídka podpisů v programu Adobe Acrobat



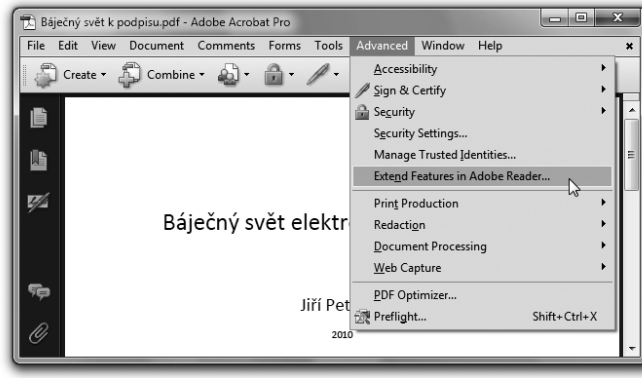
Pokud ale není podepisovaný PDF dokument vybaven formulářovým polem pro neviditelný prázdný podpis, pak význam obou popisovaných položek fakticky splývá a i volba „Podepsat dokument“ (Sign Document) vede ke vzniku viditelného podpisu.

Samotný postup při podepisování (ať již viditelným, či neviditelným podpisem) je pak již v programu Acrobat stejný, jako při podepisování pomocí Adobe Readeru. Proto si jej podrobněji popíšeme až v souvislosti s tímto programem.

6.10 Podepisování PDF dokumentů programem Adobe Reader

Program Adobe Reader od společnosti Adobe je volně šiřitelným programem, který je uživatelské veřejnosti k dispozici zdarma. Již podle svého názvu je určen ke čtení PDF dokumentů (proto: Reader). Nicméně jeho schopnosti jsou mnohem širší a lze jej využít i k podepisování PDF dokumentů. Byť jen ve smyslu „schvalovacích“ podpisů z předchozí části (a nikoli pro přidávání certifikačních podpisů či elektronických vlastnoručních podpisů, viz část 6.9.3).

Obrázek 6-84
Otevření aktuálního dokumentu pro podepisování a další úpravy v Adobe Readeru

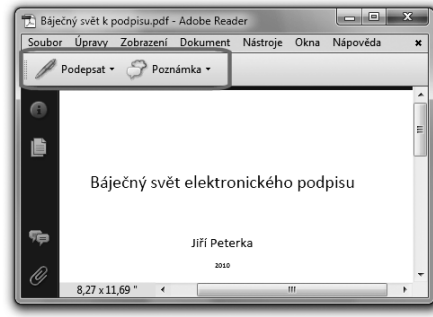


Důležité je ale to, že schopnost programu Adobe Reader je vázána na samotný podepisovaný dokument: ten musí být pro takovouto možnost speciálně upraven, jakoby „otevřen“ či „rozšířen“. K tomu je ale nutné využít (placený) program Adobe Acrobat. Konkrétní postup takového „otevření“ (rozšíření možností editace i na program Reader) v prostředí Acrobatu ukazuje předchozí obrázek.

Jakmile je takto „otevřený“ PDF dokument uložen, může být otevřen v programu Adobe Reader a v něm nejen podepisován, ale například i opatřován poznámkami.

To, že je nějaký konkrétní PDF dokument “otevřen“ pro úpravy v Adobe Readeru, se po jeho načtení v tomto programu pozná podle přítomnosti lišty s nabídkami podpisu či přidání poznámky.

Obrázek 6-85
Lišta s nabídkou podpisu signalizuje otevřený PDF dokument



Přítomnost lišty ale nemusí být směrodatná, protože její zobrazování lze vypnout. Spolehlivější je proto až možnost či nemožnost připojit podpis na aktuálně otevřený dokument: pokud je dokument otevřený, je nabídka připojení podpisu aktivní, viz následující obrázek.

Obrázek 6-86
Aktivní nabídka připojení podpisu k PDF dokumentu

Dále si připomeňme, že pokud právě zpracovávaný dokument neobsahuje žádný prázdný podpis (formulářové pole pro podpis), pak ani Adobe Reader do něj neumožní vložit neviditelný podpis, ale jen podpis viditelný. V tomto případě tedy možnosti „Podepsat dokument“ a „Umístit podpis“ splývají – a vedou na možnost připojit viditelný podpis.

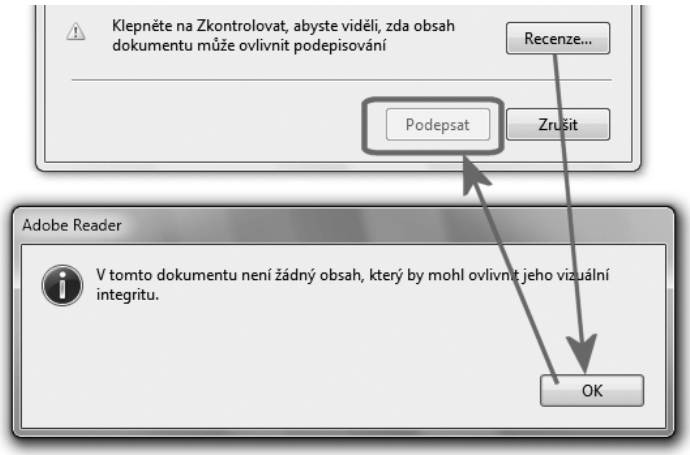
Prvním krokem při přidávání viditelného podpisu je volba oblasti, kde má být umístěn. Volí se jednoduše pomocí myši, vytvořením (libovolně velkého a libovolně umístěného) obdélníku, viz obrázek.

Obrázek 6-87
Volba oblasti pro viditelný podpis

Další kroky jsou pak již stejné pro viditelný i neviditelný podpis, byť v závislosti na nastavení: uživatel je v režimu náhledu upozorněn na případný neviditelný či aktivní obsah, který by mohl změnit vzhled podepisovaného dokumentu (podrobněji viz část 6.9.2).

Teprve když odsouhlasí, že byl seznámen s příslušným varováním, stane se tlačítko pro podpis aktivním a uživatel může skutečně připojit svůj elektronický podpis.

Obrázek 6-88
Zkontrolování obsahu, který by mohl ovlivnit vzhled podepisovaného dokumentu



6.11 PDF dokumenty „na delší dobu“

U PDF dokumentů, stejně jako snad u všech ostatních druhů elektronických dokumentů, mohou vyvstat nepříjemné problémy, pokud s nimi budeme chtít pracovat „po delší době“. Tou mohou být třeba jen měsíce, ale spíše roky, či dokonce desetiletí atd.

Jde přitom o problémy hned několika druhů. Jedním je samotná schopnost pracovat s formátem PDF: po letech již nemusíme mít k dispozici takové počítače, operační systémy a hlavně programy, které tento formát podporují.[18]

Zde si ale podrobněji všimneme jiného problému: toho, že i PDF dokumenty mohou určitým způsobem záviset na vnějších (externích) informacích a datech. Ty ale nemusí být „po delší době“ již dostupné – a bez nich není možné s PDF dokumenty plnohodnotně pracovat. O jaká externí data ale jde?

Nás zde nejvíce zajímají taková externí data, která jsou nutná k ověření elektronických podpisů na PDF dokumentech. Ale pro úplnost a vyjasnění některých důležitých souvislostí si řekněme, že jde také o data, která jsou nutná pro korektní práci s obsahem samotného PDF dokumentu, včetně zachování jeho vizuální podoby.

PDF dokumenty jsou sice poměrně „self-contained“,[19] ale nikoli úplně. Mohou například využívat externí fonty. Tedy: místo toho, aby příslušné sady písem (fonty) byly obsaženy přímo v samotném dokumentu (což nutně zvětšuje jeho velikost), jsou v dokumentu tyto fonty jen vyjmenovány a při zobrazování obsahu dokumentu se načítají „z okolního prostředí“, tj. z operačního systému.[20] Podobně může jít například o barvy a další druhy objektů, které zejména kvůli úspoře velikosti výsledného souboru nejsou vkládány přímo do něj, ale jsou přejímány z „okolního prostředí“. A pokud zde nejsou k dispozici, nastává problém.

6.11.1 „Nálepka“ PDF/A-1

Samozřejmě ale existují i určitá řešení, obvykle připravovaná pro potřeby dlouhodobé archivace PDF dokumentů. Jedním z nich je i standard PDF/A-1,[20] kde „A“ naznačuje právě archivaci. Nejde přitom o nějaký specifický formát PDF, jak je často nesprávně vnímán, ale spíše o podmnožinu jedné z verzí formátu PDF (konkrétně formátu PDF 1.4, na kterém je PDF/A-1 založen).

Nejlépe je dívat se na PDF/A-1 jako na nálepku, spojenou s definovanou „sadou restrikcí“: pokud dokument ve formátu PDF splňuje onu „sadu restrikcí“, může být opatřen nálepkou PDF/A-1.

---

18 Samozřejmě i na tento problém existuje řešení: buďto se dokumenty včas konvertují do nového formátu, nebo se vytvoří speciální programy, které simulují „původní“ prostřední a podporují i „původní“ formáty.

19 V tom smyslu, že většinu toho, co potřebují, již obsahují přímo v sobě.

20 Případně, pokud nejsou k dispozici, jsou nahrazovány (substituovány) jinými dostupnými fonty.

A o jaké restrikce se jedná? Například:

- dokument se nesmí odkazovat na žádné externí fonty; všechny fonty, které používá, v něm musí být již obsaženy
- dokument také musí obsahovat všechny definice barev, které musí být nezávislé na zařízení
- dokument musí obsahovat všechna svá metadata
- dokument naopak nesmí obsahovat:
  - žádné šifrování
  - žádnou LZW kompresi
  - žádné vložené soubory
  - žádné odkazy na vnější objekty (například URL odkazy z textu na externí webové stránky)
  - průhledné plochy (PDF Transparency)
  - multimédia
  - JavaScript

Důležité přitom je, že ani (oprávněná) existence nálepky PDF/A-1 na nějakém PDF dokumentu stále nemusí zaručovat, že s ním bude možné pracovat i „po delší době". Celá sada restrikcí tak negarantuje, ale jen zlepšuje čitelnost a možnost práce s dokumentem.[21]

„Nálepka" PDF/A-1 ale určitým způsobem souvisí i s elektronickými podpisy na PDF dokumentech. Například samotné podepisování (ani přidávání časových razítek) nezakazuje – ale říká, že by se neměla používat certifikace PDF dokumentů. Což má svou logiku: pokud je PDF/A-1 řešením pro dlouhodobou archivaci, pak u ní se nepočítá se změnami dokumentu (zatímco certifikace se od podpisu liší právě tím, že umožňuje ještě určité pozdější změny dokumentu, viz část 6.2).

Stejně tak standard PDF/A-1 nezakazuje přidávání časových razítek (ve smyslu části 6.3), ani přidávání informací o stavu revokace certifikátů (viz část 6.10). Nic z toho ale nepředepisuje, a to ani u informací o revokaci. To pak jen dokládá to, že ani získání nálepky PDF/A-1 nezaručuje úplnou nezávislost na externích informacích (protože při ověřování podpisu na dokumentu se musí získávat i externí informace o stavu revokace).

Na druhou stranu standard PDF/A-1 přeci jen určitým způsobem omezuje elektronické podepisování PDF dokumentů. Kromě toho, že zapovídá certifikační podpisy, zakazuje i takové viditelné elektronické podpisy, které pro svou vizualizaci používají takový font, který není vložen přímo do PDF dokumentu (v angličtině: není „embedded").

---

[21] Dokonce i standard PDF/A-1 má dvě různé úrovně: PDF/A-1a usiluje o co nejlepší zachování struktury PDF dokumentu, zatímco PDF/A-1b usiluje o co nejlepší zachování vizuálního vzhledu obsahu dokumentu.

6.11.2 Dokumenty PAdES

Potřebám elektronických podpisů a možnosti ověřit je i „po delší době“ se na rozdíl od standardu PDF/A specificky věnuje koncept **PAdES (PDF Advanced Electronic Signatures)**, zmiňovaný již v části 4.10.3.

Připomeňme si, že jeho podstatou je (podobně jako u PDF/A) takové přidávání původně externích informací přímo do PDF dokumentu, aby při pozdějším ověřování byly k dispozici a nemusely být načítány odněkud, kde již nemusí být dostupné. Zde konkrétně se jedná hlavně o certifikáty na celé certifikační cestě, o časová razítka, a hlavně pak o revokační informace týkající se všech certifikátů. Stejně tak si připomeňme, že celý koncept PAdES je rozdělen do několika úrovní, na kterých jsou definovány různé profily podpisů:

- **PAdES Basic** (část 2): jde o profil odpovídající „původním“ podpisům na PDF dokumentech.[22] Někdy se o profilech z této úrovně hovoří také jako o **PAdES-CMS** (či **CMS/PKCS#7**).
- **PAdES Enhanced** (část 3): zde jsou definovány profily **PAdES-BES**, **PAdES-EPES**, které již jsou založeny na konceptu CAdES. Jednotlivé podpisy dle těchto profilů mohou být opatřeny také „podpisovými“ časovými razítky, čímž se z nich stávají elektronické podpisy dle profilu **PAdES-T**.
- **PAdES Long Term** (část 4): zde je definován profil **PAdES-LTV** (někdy označovaný také jako **PAdES-A**), založený na CAdES, který umožňuje přidávat k podepsanému dokumentu samostatná („archivní“) časová razítka, za účelem zajištění časové kontinuity (ve výše uvedeném smyslu).
- **PAdES for XML Content** (část 5): zde je definován profil **PAdES-XAdES**, ve kterém lze přidávat posloupnost časových razítek k XML obsahu v rámci PDF dokumentu (například k polím formuláře, určeným k vyplňování).

V celé této kapitole jsme si až dosud popisovali vlastnosti podpisů na PDF dokumentech, které odpovídají „základní“ úrovni, neboli „části 2“ (PAdES Basic). Zdůrazněme si, že již na této úrovni je možné „prodlužovat životnost“ elektronických podpisů na PDF dokumentech, přesněji: možnost jejich ověření. A to přidávání „podpisových“ časových razítek k jednotlivým podpisům, a také přidáváním revokačních informací (CRL seznamů či odpovědí OCSP serverů), dostupným v době vzniku podpisu či „někdy později“. Viz popis v části 6.5.6.

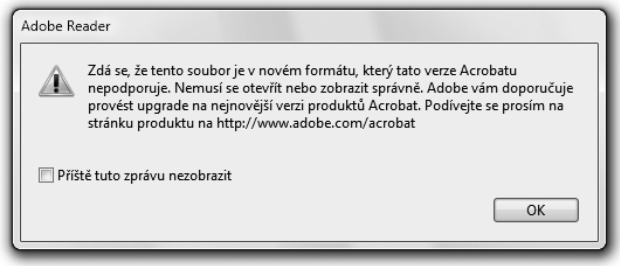
Konkrétní způsob, jakým se tak děje (jakým jsou „podpisová“ časová razítka a revokační informace přidávány do PDF dokumentu) ale na této úrovni (a u těchto podpisových profilů, tj. PAdES-CMS, resp. CMS-PKCS#7) vychází ještě z původního formátu PDF dokumentů, tak jak definován ve standardu ISO 32000.

Na úrovni PAdES Enhanced (část 3) jsou nabízeny v zásadě stejné možnosti, ale způsob ukládání dodatečných informací do PDF dokumentů je odlišný – již založený na konceptu CAdES. To má ale jeden poměrně zásadní důsledek: vzniká tím nová verze formátu PDF dokumentů, které obecně není kompatibilní s verzí předchozí. Takže novější verze programů Acrobat a Reader (konkrétně od verze X) tuto verzi podporují, ale starší verze nikoli.

---

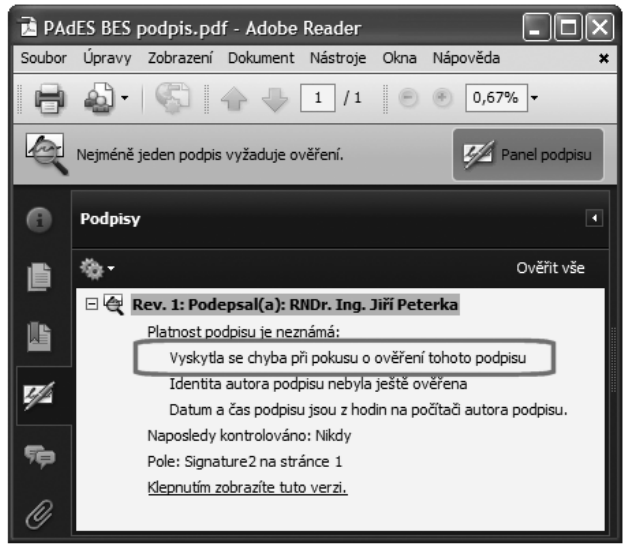
[22] Dle ISO 32000-1.

Obrázek 6-89
Hláška Acrobatu/Readeru o nepodporovaném formátu



Řečeno ještě jinými slovy: pokud v Acrobatu X či Readeru X (případně ve vyšší verzi) připojíte k PDF dokumentu nějaký podpis podle PAdES profilů z části 3 či 4, nebudou starší verze těchto produktů (Acrobat 9 a Reader 9, resp. starší) schopné s těmito podpisy pracovat. Samotný dokument PDF dokáží starší verze programů přečíst, ale podpisy a případná samostatná (archivní) časová razítka již nikoli.

Obrázek 6-90
Při pokusu o ověření (PAdES Extended) podpisu ve starší verzi Adobe Readeru je hlášena chyba



Konkrétní podpora PAdES a jeho částí v jednotlivých verzích produktů společnosti Adobe je následující:

- verze 9 podporují PAdES pouze na úrovni PAdES Basic, neboli pouze „části 2“. To znamená, že dokáže pracovat jen s podpisy na bázi profilů PAdES-CMS, označovaných také jako CMS-PKCS#7.
- verze X podporují PAdES do úrovně PAdES Long Term, neboli do části 4 (včetně). To znamená, že již podporují podpisy na bázi profilů PAdES-BES i PAdES-T z části 3 (s výjimkou profilu PAdES-EPES), a také „archivní“ časová razítka (profil PAdES-LTV, resp. PAdES-A) z části 4.

Ukažme si nyní, jak nastavit Adobe Acrobat a Reader verze 9.x tak, aby podporovaly PAdES na úrovni Basic (část 2). Pak si ukážeme, jak se nastavují stejné produkty ve verzi X, aby vytvářely podpisy buďto na úrovni Basic, nebo na úrovni Enhanced. A také jak je přimět k tomu, aby k dokumentu připojily samostatné („archivní“) časové razítko.

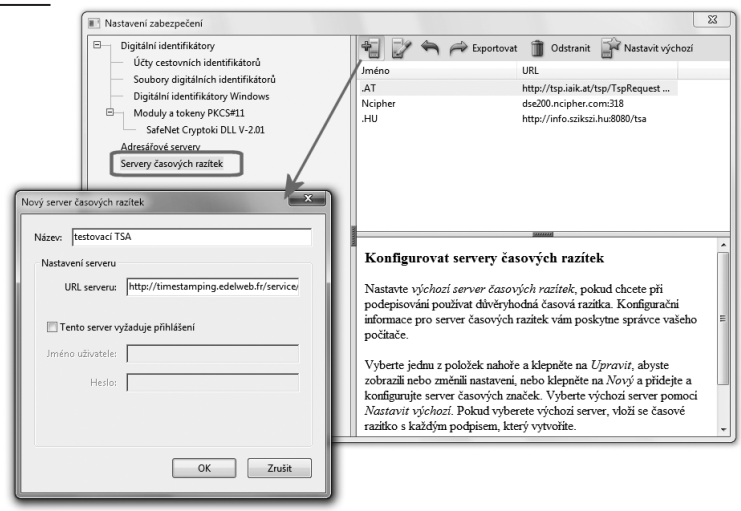
6.11.3 Nastavení Acrobatu a Readeru verze 9 pro vytváření podpisů PAdES Basic

Podle příslušného standardu[23] je elektronický podpis na úrovni PAdES Basic, neboli elektronický podpis vytvářený podle profilu PAdES-CMS (resp. SMS-PKCS#7), shodný s “běžným“ elektronickým podpisem na PDF dokumentech, tak jak jsme si jej dosud popisovali. Mělo by k němu ale být připojeno i „podpisové“ časové razítko (tedy časové razítko ve smyslu části 6.3), a také revokační informace (ve smyslu části 6.5.6). Přesněji tyto dva prvky jsou standardem doporučeny, ale nikoli striktně vyžadovány.[24]

Nastavení programu Acrobat či Reader tak, aby vytvářel podpisy dle profilů PAdES-CMS, včetně doporučených součástí, by tedy mělo zajistit oba doporučené kroky:

- přidání (podpisového) časového razítka ke každému podpisu
- přidání revokačních informací ke každému podpisu.

Obrázek 6-91
Příklad nastavení autority časového razítka



Postup přidávání (podpisových) časových razítek jsme si popsali již v části 6.9.1 (pojednávajícím o nastavení Adobe Acrobatu). Proto si jen stručně připomeňme, včetně obrázku, že fakticky jde jen o nasta-

23 ISO 32000, resp. ETSI TS 102 778.

24 Kromě toho může být (již volitelnou) součástí podpisu i důvod podpisu, umístění podpisující osoby a kontakt na ni.

vení údajů o serveru, resp. poskytovateli služby časových razítek (autoritě časových razítek, TSA). Nastavit si můžeme více takovýchto poskytovatelů, ale jednoho musíme prohlásit za „výchozího“ – a jeho časová razítka pak budou automaticky přidávána k vytvářeným podpisům.

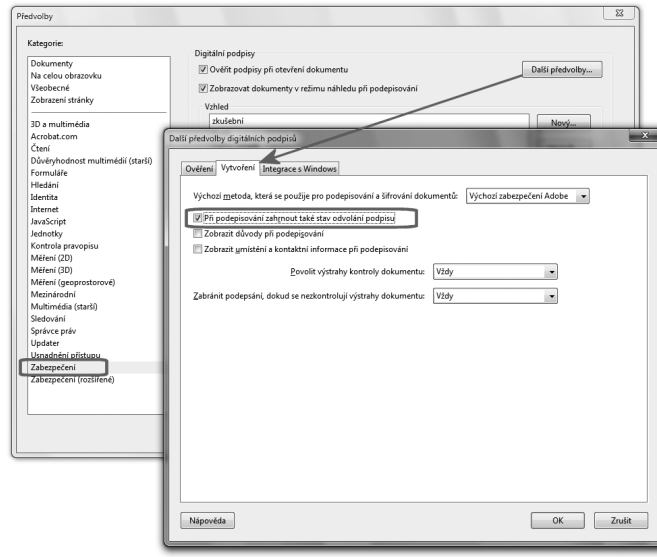
Pokud jde o informace o stavu revokace certifikátů, na kterých je podpis založen, o těch jsme si již také řekli (v části 6.5.6), že mohou být přidávány buďto v okamžiku vzniku podpisu, nebo „někdy později“. Druhý případ – přidání informací „někdy později“ – jsme si v uvedené části 6.5.6 již také popsali.

Pro přidání revokačních informací již při samotném vzniku podpisu je třeba provést příslušné nastavení v rámci předvoleb Acrobatu či Readeru, dle následujícího obrázku.

Připomeňme si ale v této souvislosti to, co jsme si zdůraznili již v části 6.5.6: jelikož tuzemské certifikační autority dosud běžně neposkytují revokační informace skrze OCSP protokol, ale jen prostřednictvím CRL seznamů, nemusí být informace o stavu revokace certifikátů v okamžiku vzniku podpisu k dispozici.

Přesněji ty informace v podobě CRL seznamu, které jsou k dispozici v okamžiku vzniku podpisu, ještě nemusí obsahovat informace o takové revokaci, ke které mohlo dojít jen několik málo hodin před okamžikem, kdy podpis vytváříme – a to kvůli tomu, že certifikační autority mají určitý čas (24 hodin) na to, aby zpracovaly žádost o revokaci a promítly ji do nově vydaného seznamu CRL.

Obrázek 6-92
Předvolba pro přidávání revokačních informací již při vzniku podpisu



Vkládání revokačních informací v okamžiku vzniku podpisu tedy není příliš výhodné, neboť pro následné ověření nepřináší dostatečnou jistotou o tom, zda některý z relevantních certifikátů nebyl v okamžiku vzniku podpisu již revokován. Výhodnější je proto přidávání revokačních informací „někdy později“ (až lze mít jistotu o tom, že příslušný seznam CRL by informaci o případné revokaci musel obsahovat).

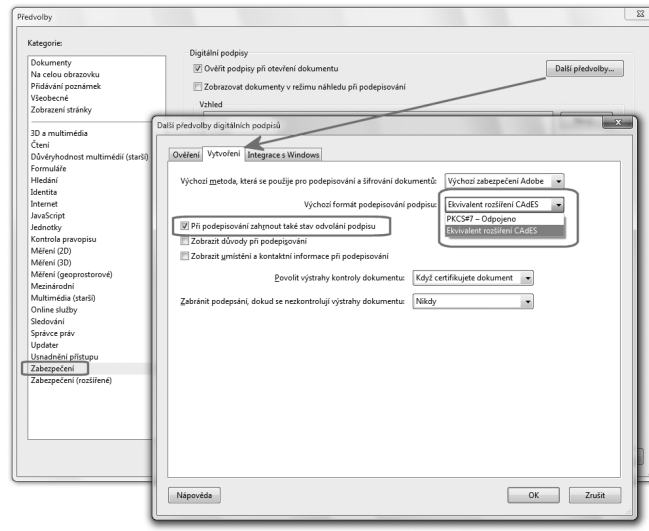
6.11.4 Nastavení Acrobatu a Readeru verze X pro vytváření podpisů PAdES

V případě programů Acrobat a Reader verze X je základ nastavení v zásadě obdobný: je třeba ošetřit přidávání revokačních informací (buďto automaticky, při vytváření podpisu), případně „někdy později“. Stejně tak je třeba nastavit autoritu časového razítka.

Specifikem verze X je ale volba mezi úrovní PAdES Basic (resp. částí 2) a PAdES Enhanced (část 3). V závislosti na tom pak jsou jednotlivé elektronické podpisy na dokumentu vytvářeny podle profilů PAdES-CMS (resp. CMS-PKCS#7), nebo podle profilu PAdES-BES.

Možnost volby mezi těmito dvěma úrovněmi ukazuje následující obrázek. Od předchozího se liší v zásadě jen novým prvkem pro „Výchozí formát podepisování podpisu“, umožňujícím zvolit jednu z obou možných úrovní: Basic (prezentovanou jako „PKCS#7”) a Enhaced (prezentovanou jako „Ekvivalent rozšíření CAdES“).

Obrázek 6-93
Nastavení Acrobatu/Readeru pro vytváření PAdES podpisů



Připomeňme si znovu, že pokud bude nastavena úroveň „Enhanced“ (resp. „Ekvivalent rozšíření CAdES“), bude následně podepsaný dokument uložen do nové verze PDF formátu, kterou starší verze programů (Acrobat a Reader 9 a starší) sice dokáží přečíst, ale nedokáží pracovat se samotným podpisem.

Na obou úrovních, tedy jak Basic tak Enhanced, mohou být k jednotlivým elektronickým podpisům přidávána („podpisová“) časová razítka. Děje se tak v závislosti na nastavení autority časových razítek, způsobem popsaným v části 6.9.1. Proto jen stručně pro připomenutí: jeden z nastavených serverů, poskytujících časová razítka, musí být prohlášen za výchozí. Teprve pak jsou časová razítka k podpisům skutečně přidávána (jako „podpisová“).

Nastavením výchozího poskytovatele (serveru) časových razítek se současně rozhoduje o tom, zda na úrovni PAdES Enhanced budou jednotlivé podpisy vytvářeny podle profilu PAdES-BES (bez časového razítka), nebo dle profilu PAdES-T (s „podpisovým“ časovým razítkem, které je pro úroveň PAdES Enhanced doporučeno, nikoli ale striktně vyžadováno).

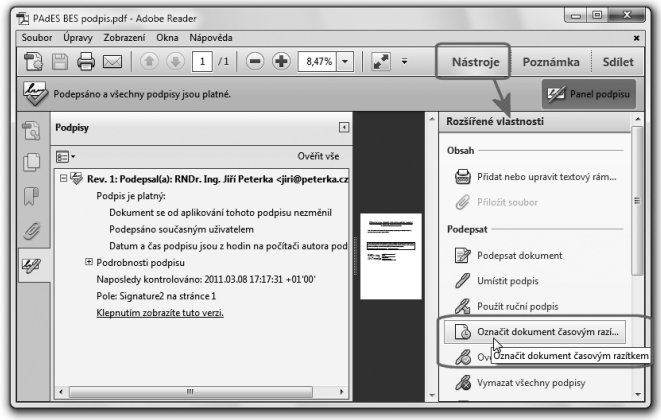
6.11.5 Přidávání „archivních“ časových razítek k PDF dokumentům

Připomeňme si, že Adobe Acrobat i Reader do verze 9 (včetně) pracují pouze s časovými razítky, která nejsou samostatná, ale jsou spojena s konkrétním elektronickým podpisem do té míry, že se jeví jako jeho atribut (jako důvěryhodný způsob získání časového údaje, který je přímou součástí elektronického podpisu). Sama společnost Adobe o těchto časových razítkách hovoří jako o „podpisových“.

Konkrétní vlastností těchto „podpisových“ časových razítek je i to, že ke každému podpisu může být připojeno vždy nejvýše jedno takové časové razítko (nebo žádné). Není možné přidávat k jednotlivým podpisům – ale ani k celému PDF dokumentu jako takovému – další časová razítka, pro potřeby zajištění digitální kontinuity. Místo toho by bylo nutné přidávat vždy nový elektronický podpis (a teprve s ním další časové razítko).

Možnost přidávat k PDF dokumentům další, a to již samostatná časová razítka, se objevuje až ve verzi X programů Acrobat a Reader, v souvislosti s podporou konceptu PAdES. Konkrétně jeho úrovně „Long Term“ (neboli „části 4“ standardu), na které je definován profil PAdES-LTV. Ten je někdy označován také jako PAdES-A, kde písmeno A naznačuje využití pro „archivní“ účely.

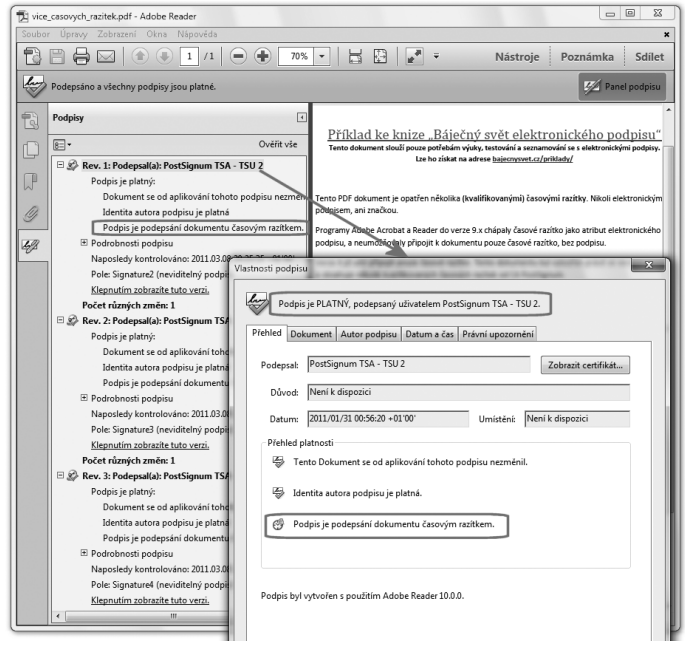
Takovýchto „archivních“ časových razítek, na bázi profilu PAdES-LTV resp. PAdES-LTV, je možné přidávat k jednomu PDF dokumentu více, apriorně neomezeně, s libovolnými časovými odstupy. Je tedy možné tato časová razítka řetězit (přidávat nové ještě dříve, než skončí možnost ověření toho předchozího), a tím „prodlužovat život“ PDF dokumentům (prodlužovat možnost ověření jejich podpisů).



Obrázek 6-94
Přidání samostatného (archivního) časového razítka k PDF dokumentu

Zajímavé je, že Adobe Reader (i Acrobat) zobrazují takovéto „archivní“ razítko stejně jako další elektronický podpis, jen s poněkud odlišnou ikonkou. Jako autora takovéhoto podpisu prezentují tu autoritu, která poskytla časové razítko (zřejmě přebírají její jméno z certifikátu, na kterém je razítko založeno). A v české lokalizaci je k popisu časového razítka přidávána ještě poněkud nesmyslná formulace „Podpis je podepsání dokumentu časovým razítkem“. Příklad, s několika časovými razítky, ukazuje následující obrázek.

Obrázek 6-95
Příklad PDF dokumentu s více samostatnými (archivními) časovými razítky, v Adobe Readeru X

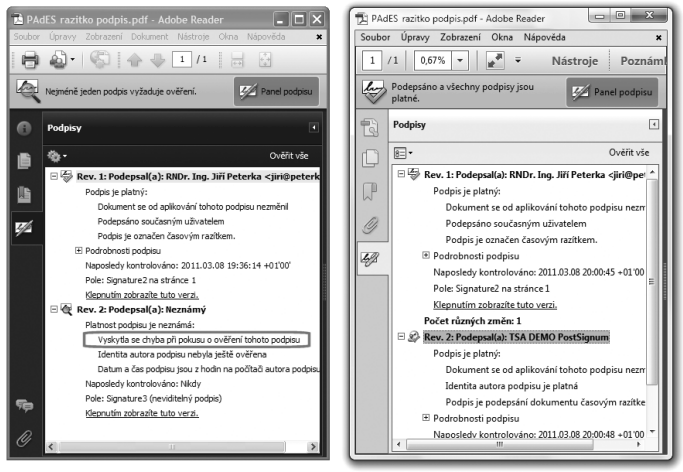


Jakmile je ale k PDF dokumentu přidáno první samostatné časové razítko, může být dokument uložen již jen do nového PDF formátu – se všemi důsledky, které to má pro zpětnou kompatibilitu.

Konkrétně to znamená, že samotný PDF dokument bude ve starších verzích programů Acrobat a Reader (verze 9 a starších) běžně čitelný, byť s úvodním hlášením o novém a nepodporovaném formátu. Nicméně samostatné časové razítko nebude korektně čitelné, takže při pokusu o jeho ověření bude hlášena chyba. Stejně jako pro podpisy, vytvořené na úrovni Enhanced, neboli podle profilů PAdES-BES (či PAdES-T, včetně „podpisového“ časového razítka).

Příklad ukazuje následující obrázek, na kterém je jeden a tentýž soubor – s jedním „starším“ podpisem dle PAdES-CMS (s „podpisovým“ časovým razítkem) a jedním samostatným (archivním) časovým razítkem. Vpravo je platnost podpisu a samostatného razítka korektně vyhodnocena v Adobe Readeru verze X, zatímco vlevo je pokus o totéž ve verzi 9: podpis byl korektně vyhodnocen, zatímco při pokusu o vyhodnocení samostatného (archivního) časového razítka se vyskytla chyba.

Obrázek 6-96
Vyhodnocení platnosti v Adobe Readeru verze 9 (vlevo) a verze X (vpravo)



Jak je z levé části obrázku patrné, Readeru verze 9 se nepodařilo ani získat základní údaje z certifikátu, na kterém je časové razítko založeno. Proto nejen že neříká, kdo časové razítko vystavil – ale dokonce ani nenaznačuje, že se jedná o časové razítko a nikoli o elektronický podpis.

7. Elektronický podpis v MS Office

Kapitola 7

7. Elektronický podpis v MS Office

Podpora elektronických podpisů je standardně zabudovávána i do nejrůznějších dalších softwarových aplikací, které slouží k práci s dokumenty v elektronické formě. Nejinak je tomu i v případě kancelářského balíku MS Office.

Míra této podpory se ale u jednotlivých verzí MS Office zásadně liší jak podle verze celého balíku, tak i podle toho, zda jde o podepisování dokumentů (například programem MS Word), nebo o podepisování e-mailových zpráv (programem MS Outlook).

Možnost elektronického podepisování dokumentů byla poprvé zavedena u verze MS Office 2002/XP, zůstala stejná i u verze 2003 a byla velmi nedokonalá: pro ukládání (interních) elektronických podpisů do jednotlivých dokumentů byl používán vlastní (proprietární) binární formát, podporována byla pouze hašovací funkce SHA-1, a hlavně zde nedocházelo k plnohodnotnému ověřování (vyhodnocování platnosti) elektronických podpisů, když se kontrolovala pouze integrita podepsaného dokumentu.

Teprve verze MS Office 2007 přinesla plnohodnotnou práci s elektronickými podpisy. Pro své dokumenty zavedla formát založený na XML, a pro ukládání elektronických podpisů do těchto dokument začala používat standard XML-DSig.

Kromě neviditelných podpisů zavedla i podpisy viditelné, v obdobném smyslu jako na PDF dokumentech. Dokáže již pracovat s hašovací funkcí SHA-2, a hlavně již vyhodnocuje platnost elektronických podpisů i s uvážením řádné platnosti certifikátů a stavem jejich revokace. Stále však neumožňuje připojovat k elektronickým podpisům například časová razítka, případně další revokační informace.

S výraznou inovací přišla verze MS Office 2010, která zavedla podporu možnosti dlouhodobějšího ověřování elektronických podpisů (LTV, Long Term Validation), tak jak jsme si ji popisovali v části 4.10.3 – a to pomocí implementace konceptu XAdES, jako rozšíření používaného formátu XML-DSig.

Pokud jde o podepisování (e-mailových) zpráv, to se objevuje již v rámci programu MS Outlook ve verzi 2000, a postupně se zdokonaluje. Ani verze MS Outlook 2010 však nepodporuje koncept XAdES, a tudíž neumožňuje k podepisovaným zprávám připojovat například časová razítka atd.

V této kapitole si podrobněji popíšeme způsob práce s elektronickými podpisy jak na dokumentech, tak i na zprávách elektronické pošty. V prvním případě (u dokumentů) na konkrétním příkladu programu MS Word ve verzích2003, 2007 a 2010. Možnost podepisování e-mailových zpráv, programem MS Outlook, se naopak s postupujícími verzemi MS Office prakticky neměnila. A tak si vše ukážeme podrobněji jen na verzi MS Outlook 2010.

Popisovat si přitom budeme chování standardních „krabicových“ produktů, tak jak jsou nastaveny od výrobce, resp. jak se samy nastaví při běžné instalaci u koncového uživatele.

Pouze tam, kde to bude nezbytné, si ukážeme, jak se standardní chování programů z balíku MS Office dá měnit prostřednictvím různých speciálních nastavení, určených správcům.[1]

7.1 Elektronické podpisy v programu MS Word XP a 2003

Možnost elektronicky podepsat dokument (byť prezentovaná jako možnost přidat digitální podpis) se v rámci balíku MS Office objevuje až od jeho verze 2002 (MS Office 2002, známější spíše jako MS Office XP) a týká se jak editoru MS Word, tak i spreadsheetu Excel a programu PowerPoint. Stejné vlastnosti pak měla i verze MS Office 2003.

Jednalo se ale ještě o velmi zjednodušenou podporu elektronických podpisů, kterou z dnešního pohledu nemůžeme považovat za dostatečnou pro práci se zaručenými elektronickými podpisy. Však také tehdejší aplikace samy přinášely v tomto ohledu výmluvný disclaimer, který vidíte na obrázku.

Obrázek 7-1
Disclaimer o právní nezávaznosti podpisu v MS Office XP/2003

Důvodem byla především skutečnost, že tyto verze MS Office (tj. XP a 2003) vyhodnocovaly pouze integritu elektronicky podepsaného dokumentu, ale již nebraly ohled na řádnou dobu platnosti či stav revokace certifikátu, na kterém je podpis založen, a ani se nesnažily hodnotit platnost či neplatnost podpisu jako takového.

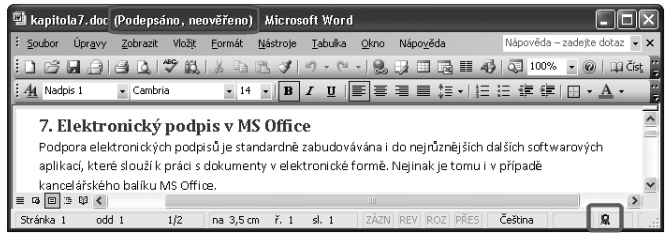
Stejně tak tyto verze MS Office používaly svůj vlastní (proprietární a binární) datový formát jak pro ukládání samotných dokumentů, tak i pro vkládání elektronických podpisů do těchto dokumentů.

[1] Tato nastavení si budeme popisovat raději skrze přímé nastavení položek tzv. registru, protože u verzí produktů určených běžným uživatelům nemusí být k dispozici nástroje pro jejich snazší nastavování (jako jsou nástroje pro práci se zásadami skupiny či tzv. Office Customization Tool).

7.1.1 Ověřování podpisů

To, že nějaký dokument je opatřen elektronickým podpisem, indikoval program MS Word verze XP či 2003 malou červenou ikonkou, umístěnou v pravé části spodního (stavového) řádku, viz obrázek. Poklepání na tuto ikonku bylo současně příkazem k ověření, resp. vyhodnocení elektronického podpisu (či podpisů) na dokumentu.

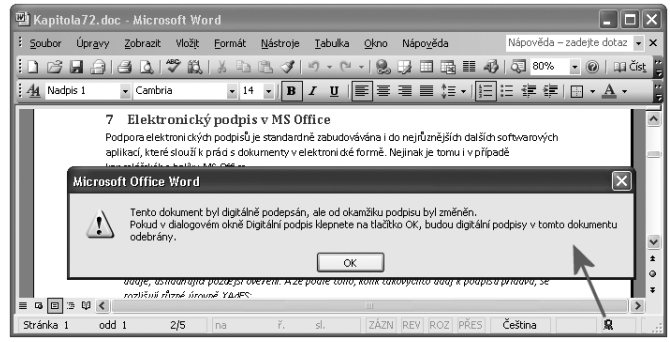
Obrázek 7-2
Indikace elektronicky podepsaného dokumentu v programu MS Word



Druhým indikátorem toho, že dokument je podepsán, byl nápis „Podepsáno, neověřeno“ v záhlaví okna programu MS Word. Tento indikátor byl ale zobrazován jen do doby, než došlo k vyhodnocení elektronického podpisu – které, jak jsme si již řekli, obnášelo jen ověření integrity podepsaného dokumentu.

V případě, kdy integrita podepsaného dokumentu byla porušena, byla uživateli místo okna s výčtem podpisů zobrazena hláška o změně dokumentu od jeho podepsání, viz následující obrázek.

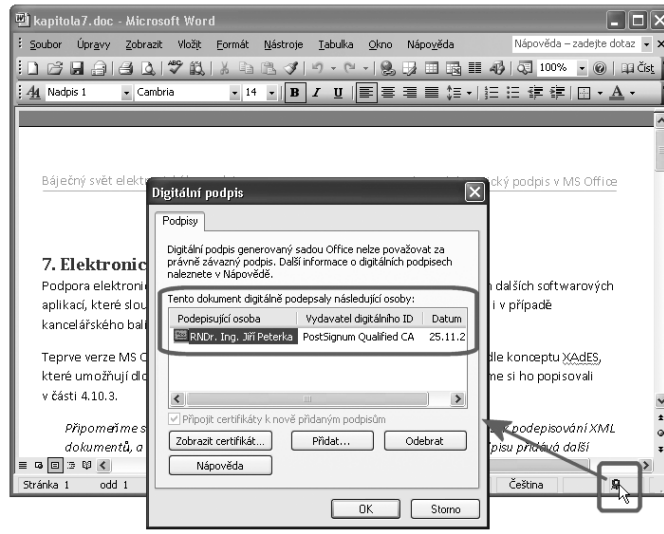
Obrázek 7-3
Příklad hlášky o porušené integritě dokumentu



V případě, kdy integrita podepsaného dokumentu porušena nebyla, bylo uživateli zobrazeno standardní okno s výčtem elektronických podpisů, připojených k dokumentu – ovšem bez jakékoli indikace či sdělení ohledně toho, zda konkrétní podpis je či není platný.

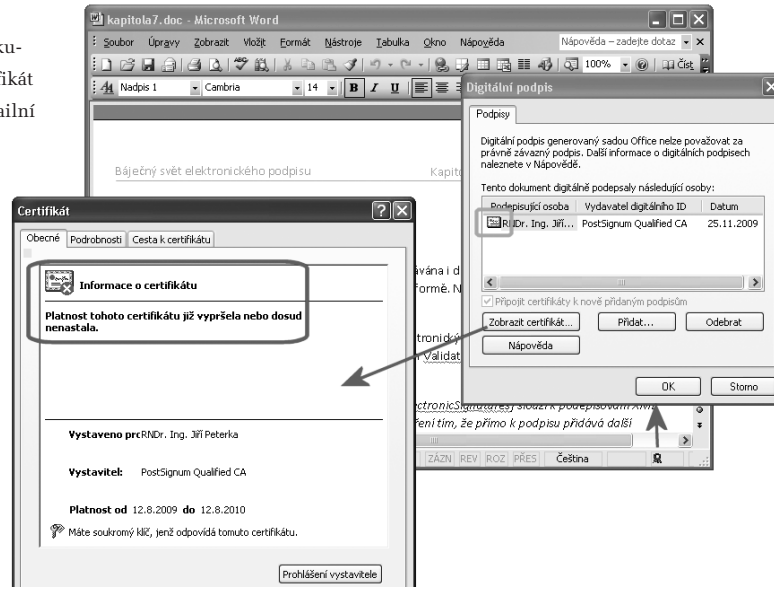
Pokud uživatel chtěl, mohl si nechat zobrazit stav příslušných certifikátů a podle něj si sám odvodit stav platnosti celého podpisu.

Obrázek 7-4
Výčet podpisů na dokumentu s neporušenou integritou



Vyhodnocení platnosti certifikátů přitom probíhalo skrze mechanismy, které se starají o certifikáty v systémovém úložišti certifikátů MS Windows. Tyto mechanismy vyhodnocovaly platnost certifikátu a mohly ověřit i stav revokace certifikátu.

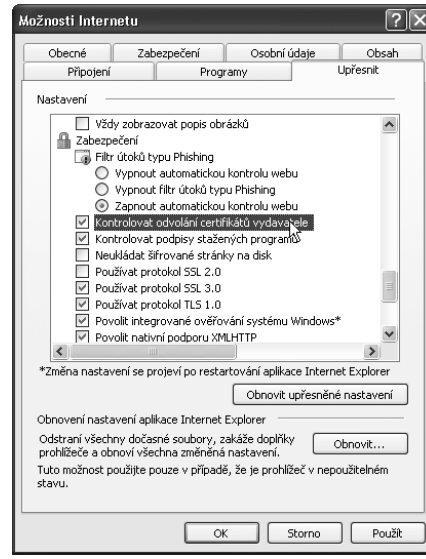
Obrázek 7-5
Informace o existenci podpisu na dokumentu (vpravo) nenaznačují, že certifikát již není platný – toto odhaluje až detailní pohled na samotný certifikát



K tomu ale bylo nutné příslušnou možnost nejprve zapnout, a to v rámci nastavení prohlížeče Internet Explorer – protože u dřívějších verzí byla standardně vypnutá.

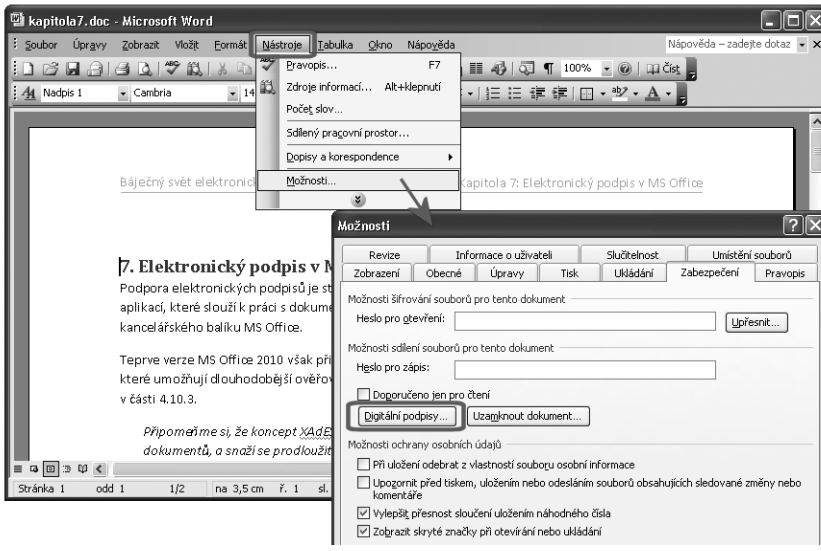
Obrázek 7-6

Volba kontroly revokace



Obrázek 7-7

Způsob vkládání elektronických podpisů do dokumentů v programu MS Word verze 2003

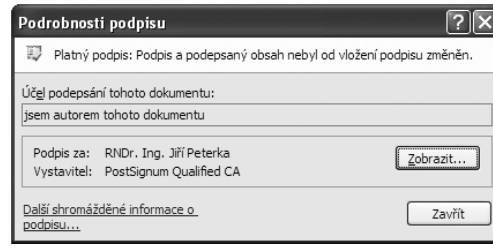


Samotné přidání elektronického podpisu se v programu MS Word verze 2002/XP a 2003 provádělo nejjednodušeji přes menu: přes položku Nástroje v hlavním menu, pak volbu Možnosti, a pak přes záložku Zabezpečení. Na té se již nacházelo tlačítko pro přidání elektronických (resp. digitálních) podpisů, stejně tak jako případných hesel pro zamykání souboru, viz předchozí obrázek.

7.2 Elektronické podpisy v programu MS Word 2007

Podstatně lepší implementace se elektronické podpisy (na dokumentech) dočkaly v kancelářském balíku MS Office 2007, opět v rámci programů Word, Excel a PowerPoint. Kromě zásadní změny uživatelského rozhraní (které s elektronickými podpisy přímo nesouvisí) došlo k přechodu na XML formáty při ukládání dokumentů, a na standard XML-DSig pro vkládání elektronických podpisů do těchto dokumentů. Dále přibyla podpora viditelných podpisů,[2] a také podpora hašovací funkce SHA-2. Ta je ale implicitně vypnuta, takže bez aktivního přenastavení[3] jsou dokumenty stále podepisovány s využitím hašovací funkce SHA-1.

Obrázek 7-8
Hodnocení platnosti podpisu v MS Word 2007



Stále však chybí schopnost práce s časovými razítky, což znemožňuje práci s elektronickými podpisy v delším časovém horizontu (po skončení řádné platnosti jejich podpisového certifikátu).

Zmizel již také původní disclaimer o „právní nezávaznosti podpisů“ (viz předchozí část) a jednotlivé programy (Word, Excel a Powerpoint) již začaly ověřovat platnost jednotlivých podpisů. Takže již neuvádí pouhý výčet podpisů, připojených k dokumentu, ale vyjadřují se i k jejich platnosti. Konkrétní hláška, kterou vidíte na obrázku, sice ještě naznačuje, že by mohla být kontrolována jen integrita dokumentu (viz „podpis a podepsaný obsah nebyl od vložení podpisu změněn“).

Ve skutečnosti je ale do hodnocení platnosti podpisu již zahrnuto i hodnocení platnosti certifikátu, na kterém je podpis založen, a také všech nadřazených certifikátů.

[2] Kterou si popíšeme až pro verzi 2010.

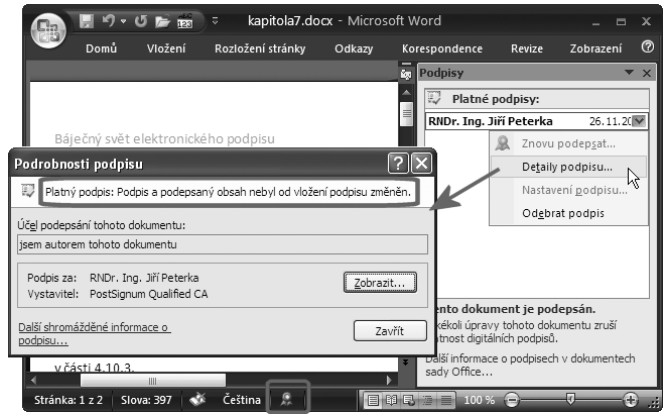
[3] Konkrétní postup viz část 7.5.2.

7.2.1 Ověřování podpisů

To, že je nějaký konkrétní dokument elektronicky podepsán, se u verze 2007 opět pozná zejména podle stejné ikony (a na stejném místě, ve spodním stavovém řádku), jako u předchozích verzí. Nyní ale k vyhodnocení platnosti podpisů dochází automaticky již při otevírání dokumentu v editoru MS Word – a nikoli až poklepáním na tuto ikonku. Naopak chybí možnost nechat si vyhodnotit platnost podpisu na vlastní popud (kdykoli později).

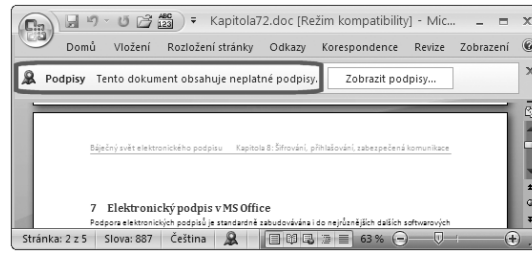
Poklepání na ikonu (stylizovanou do tvaru pečeti) nyní pouze otevře samostatné boční okno, které ukáže přehled všech podpisů, kterými je dokument opatřen. Přes rozbalovací menu u každého podpisu (přes pravé tlačítko) je pak nabídnuta možnost zobrazení podrobnějších informací o konkrétním podpisu, informací o jeho nastavení (u viditelných podpisů), i možnost jeho odstranění, viz obrázek.

Obrázek 7-9
Indikace podepsaného dokumentu a zobrazení informací o podpisu



Pokud je s elektronickým podpisem na dokumentu nějaký problém, je tato skutečnost zjištěna ihned při otevření dokumentu (v rámci ověřování), ještě než má uživatel možnost cokoli s dokumentem udělat. Pod hlavním menu je v takovém případě ihned zobrazena nová lišta informující o problému, viz následující obrázek.

Obrázek 7-10
Konstatování neplatnosti podpisu (či podpisů) na dokumentu

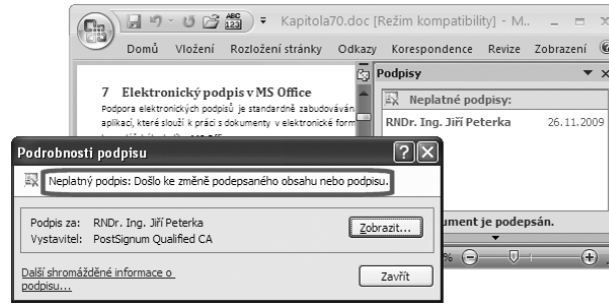


Podpis, který nemohl být vyhodnocen jako platný, je na této liště ihned prezentován jako neplatný. To proto, že MS Word 2007 formálně rozlišuje jen dva možné stavy podpisů na dokumentech: **platný** a **neplatný.**

U těch podpisů, které označí jako neplatné, ale MS Word 2007 přesto detailněji rozlišuje důvody, kvůli kterým je vyhodnotil jako neplatné. Pokud na uvedené liště zvolíte „Zobrazit podpisy" a necháte si zobrazit detaily o takovém podpisu, můžete se s těmito důvody seznámit. A MS Word vám sám naznačí, zda je podpis skutečně neplatný, nebo zda je s ním nějaký jiný problém, který by měl správně vyústit v hodnocení „nevím".[4]

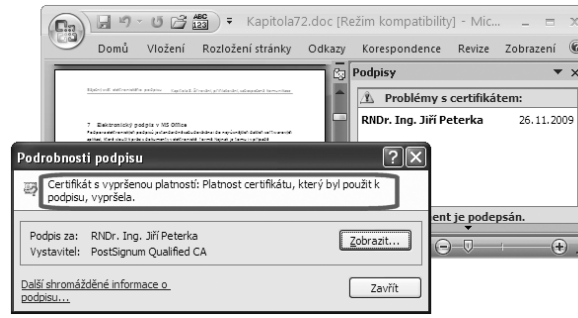
Příkladem může být podpis na dokumentu s porušenou integritou. Zde MS Word sám (v okně s detaily podpisů) zopakuje, že jde o neplatný podpis, a použije k tomu červenou barvu a ikonku s červeným křížkem, viz obrázek.

Obrázek 7-11
Skutečně neplatný podpis z důvodu porušení integrity



Jindy ale sám popře své celkové hodnocení toho, že podpis je neplatný. Například když důvodem je skončení řádné platnosti certifikátu, na kterém je podpis založen. Při zobrazení detailnějších informací o podpisu pak MS Word 2007 sám správně naznačí, již bez použití červené barvy, že jde jen o „problém s certifikátem", který nemusí zakládat (a také nezakládá) neplatnost podpisu.

Obrázek 7-12
Podpis založený na certifikátu, kterému již skončila jeho řádná platnost

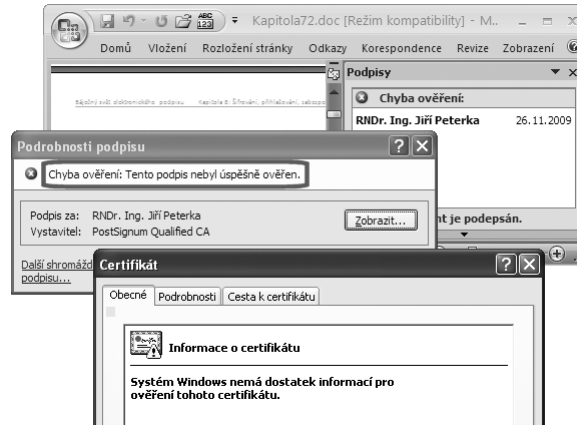


> Příklad ukazuje předchozí obrázek: je na něm dokument, podepsaný 26. 11. 2009, a jeho podpis je založen na certifikátu, který byl platný do 12. 8. 2010. Vyhodnocování ale bylo prováděno k pozdějšímu okamžiku, kdy již řádná platnost certifikátu skončila.

Poměrně specifickou hlášku má MS Word 2007 i pro situaci, kdy nedokáže vyhodnotit platnost elektronického podpisu kvůli tomu, že nemá k dispozici některý z jeho nadřazených certifikátů. Zde výsledek klasifikuje jako „chybu ověření“. Ovšem o důvodech, resp. o příčině chyby, se lze dozvědět až pohledem na certifikát, na kterém je podpis založen.

> Příklad ukazuje následující obrázek: je na něm dokument, podepsaný 26.11.2009, a vyhodnocovaný ještě v době platnosti certifikátu, na kterém je tento podpis založen (posunutím hodin na počítači). Z používaného úložiště certifikátů byl ale odstraněn kořenový certifikát autority, která tento certifikát vydala (a který se automaticky nedočítá).

Obrázek 7-13
Vyhodnocení podpisu v situaci, kdy není k dispozici kořenový certifikát autority



Verdikt ve smyslu „chyby ověření“ je v daném případě formálně správný, protože vyhodnocení (ověření) se skutečně nemohlo provést. Ani tento fakt ale neznamená, že by příslušný podpis mohl být celkově shledán neplatným. Z hlediska platnosti posuzovaného podpisu by správně mělo jít o stejný výsledek jako u předchozího příkladu (s již neplatným certifikátem), a to ve smyslu „nevím“ (viz kapitola 3). Nicméně MS Word v obou případech hodnotí podpis celkově jako neplatný.

Nesprávný je také standardní (default) způsob, jakým MS Word 2007 (a obecně i další programy z balíku MS Office 2007, s drobnou výjimkou programu Outlook) vyhodnocuje stav revokace certifikátů.[5]

[4] Ve smyslu pravidel pro ověřování elektronických podpisů, popisovaných v kapitole 3.

[5] Toto standardní chování je možné měnit (prostřednictvím nastavení v registru) jen u programu MS Outlook.

Snaží se sice získat potřebné revokační informace (seznamy CRL) a vyhodnocuje je, ale pouze pokud je online a má funkční přístup k Internetu. To znamená, že jeden a tentýž elektronický podpis na témže dokumentu může vyhodnotit (ke stejnému časovému okamžiku) jako platný nebo naopak jako neplatný podle toho, zda právě má možnost si stáhnout příslušný CRL seznam či nikoli.

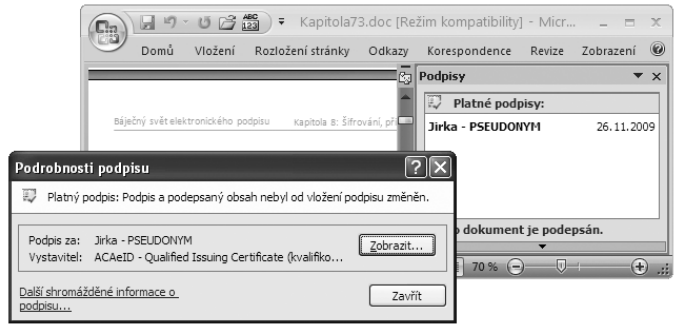
MS Word přitom dokáže pracovat i s verzemi CRL seznamů, které byly staženy někdy dříve, jsou uloženy ve vyrovnávacích (cache) pamětech operačního systému, a jsou stále platné.

Nicméně ve svém standardním nastavení MS Word 2007 uživateli nedává najevo (nesignalizuje), zda v době vyhodnocování podpisu měl potřebné revokační informace k dispozici a využil je, nebo nikoli. Což z pohledu uživatele znamená, že prakticky nemůže rozlišit oba možné, ale zásadně odlišné výsledky vyhodnocení platnosti podpisu.

Konkrétní příklad ukazují následující dva obrázky: je na nich stejný dokument opatřený stejným elektronickým podpisem, který je založen na revokovaném certifikátu (přesněji: revokovaném k okamžiku, který s dostatečným předstihem předcházel okamžiku, ve kterém je vyhodnocení prováděno).

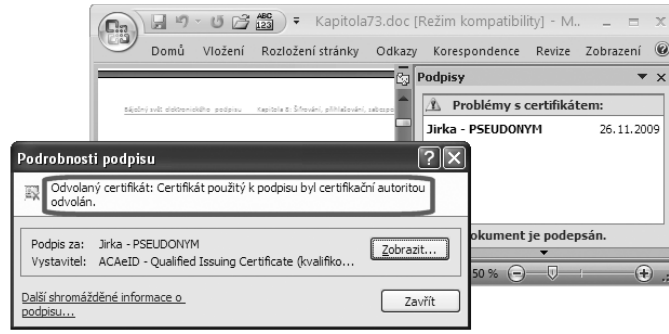
> První obrázek ukazuje situaci, kdy MS Word (resp. počítač, na kterém běží) neměl přístup k Internetu (nebyl on-line) a neměl k dispozici ani žádnou dřívější verzi CRL seznamu, ze které by se dozvěděl, že příslušný certifikát byl revokován. Proto shledal podpis platným. Nic ale uživatele nevaruje před tím, že nebyla ověřena případná revokace certifikátu.

Obrázek 7-14
Podpis, založený na revokovaném certifikátu, byl vyhodnocen jako platný



> Druhý obrázek ukazuje situaci, kdy MS Word 2007 (resp. počítač) již měl přístup k Internetu a mohl si tak stáhnout aktuální seznam CRL (nebo mohl využít některou dříve získanou a ve vyrovnávací paměti uloženou verzi CRL seznamu). Zde již správně konstatoval, že podpis je neplatný (protože je založen na revokovaném certifikátu).

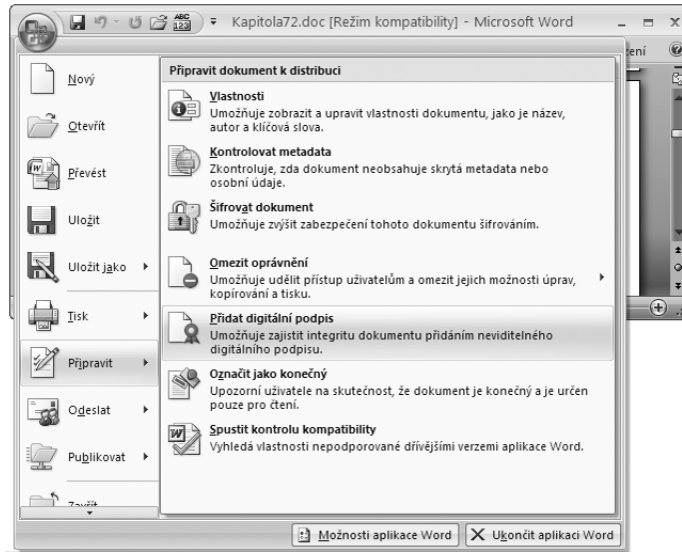
Obrázek 7-15
Podpis, založený na revokovaném certifikátu, již nebyl vyhodnocen jako platný



7.2.2 Vytváření podpisů

Vytváření, resp. přidávání elektronických podpisů k dokumentům pomocí programu MS Word verze 2007 je poměrně jednoduché a přímočaré. Nejsnazší je kliknout na nové „Office tlačítko“ (v levém horním rohu) a z následné nabídky volit možnost „Připravit“. Zde již jedna z možností přímo nabízí „Přidat digitální podpis“ (neboli, ve zde používané terminologii, podpis elektronický).

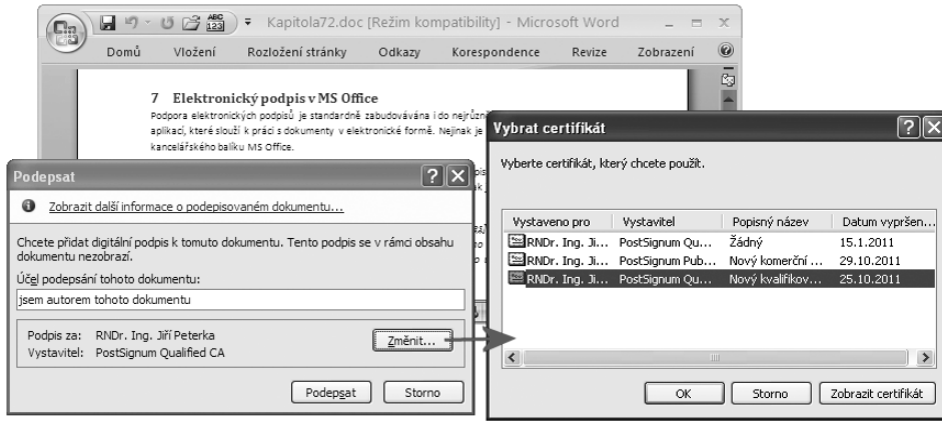
Obrázek 7-16
Přidání elektronického podpisu k právě otevřenému dokumentu



Následně je uživateli zobrazeno okno s příznačným názvem „Podepsat“, které umožňuje vyplnit důvod podpisu a také vybrat certifikát, na kterém má být podpis založen.

Obrázek 7-17

Samotné podepisování v programu MS Word verze 2007



K dispozici jsou přitom ty osobní certifikáty, které jsou umístěny v systémovém úložišti certifikátů MS Windows (nebo jsou do něj právě „promítnuty“ z některého externího úložiště, například na čipové kartě či USB tokenu), jsou aktuálně platné a je k nim k dispozici odpovídající soukromý klíč.

7.3 Elektronické podpisy v programu MS Word 2010

Nejnovější verze kancelářského balíku MS Office výrazným způsobem rozšiřuje svou podporu elektronických podpisů na objektech charakteru dokumentů. Tedy nejen na textových dokumentech, zpracovávaných programem MS Word, ale i na spreadsheetech, zpracovávaných v Excelu či prezentacích, zpracovávaných programem PowerPoint.

Asi největší změnou je zavedení podpory konceptu XAdES pro elektronické podpisy (jako rozšíření formátu XML-DSig, používaného již ve verzi 2007). To již umožňuje připojovat k podpisům na dokumentech MS Office časová razítka, ale kromě toho i další informace týkající se revokace. To pak umožňuje vyhodnocování a ověřování podpisů i po delší době, kdy již skončila řádná platnost podpisového certifikátu.

> Podpora konceptu XAdES se ale stále netýká programu MS Outlook 2010.

Podpora konceptu XAdES se v rámci Office 2010 týká jak neviditelných podpisů, tak i podpisů viditelných (zavedených již ve verzi 2007, v podobném významu v jakém fungují u PDF dokumentů). Viditelné podpisy je v Office 2010 možné přidávat k dokumentům v programech Word, Excel a InfoPath (ale nikoli k prezentacím v programu Powerpoint).

Obecně však podpora XAdES není zpětně kompatibilní s předchozími verzemi MS Office.

Základní pravidla a postupy vyhodnocování platnosti (ověřování) elektronických podpisů jsou obdobné jako u verze 2007. Novinkou je ale rozlišování tří možností stavu podpisu, kdy vedle platného a neplatného podpisu je uvažována ještě „zotavitelná chyba" ověření.

Vedle toho byly mechanismy ověřování doplněny o to, co souvisí s novými schopnostmi, včetně podpory XAdES. Takže při ověřování se uživatel mj. dozví, o jakou úroveň XAdES podpisu se jedná.

7.3.1 Podpora XAdES

Připomeňme si, že koncept **XAdES (XML Advanced Electronic Signatures)** je rozšířením standardu XML-DSig, který slouží k podepisování XML dokumentů (a který MS Office používá již ve verzi 2007). Snaží se prodloužit možnost ověření podpisů tím, že k nim přidává další údaje, usnadňující pozdější ověření. A že podle toho, kolik takovýchto údajů k podpisu přidává, se rozlišují různé úrovně XAdES:

1. základní úroveň **XAdES**: nepřidává nic (tedy ani časové razítko). Někdy je tato úroveň označována také jako XAdES-BES či EPES[6]
2. úroveň **XAdES-T** (Timestamp): přidává právě časové razítko
3. úroveň **XAdES-C** (Complete): přidává odkazy na všechny certifikáty na certifikační cestě a odkazy na všechny revokační informace.
4. úroveň **XAdES-X** (eXtended): slučuje obě předchozí varianty, tj. přidává odkazy na certifikáty na certifikační cestě a na revokační informace (jako u úrovně C) a přidává časové razítko (jako u úrovně T)
5. úroveň **XAdES-X-L** (eXtended Long term): k podpisu jsou připojeny samotné certifikáty na certifikační cestě a revokační informace (nikoli jen odkazy na ně), a také časové razítko.
6. úroveň **XAdES-A** (Archival): na této úrovni může být k podpisu přidávána ještě posloupnost dalších časových razítek, které zajišťují dlouhodobou kontinuitu.

MS Office 2010 ale neimplementuje celý rozsah konceptu XAdES, resp. všechny jeho úrovně — chybí mu podpora pro nejvyšší úroveň A (Archival).

Navíc je podpora XAdES (do úrovně X-L) omezena jen na programy Word, Excel, PowerPoint a InfoPath.

V praxi to znamená, že k jednotlivým dokumentům, zpracovávaným v programech Word, Excel, Powerpoint či InfoPath verze 2010, již je možné přidávat časová razítka a také všechny certifikáty a revokační informace, ať jde o CRL seznamy či odpovědi OCSP serverů. Co stále možné není, je přidávání posloupnosti časových razítek, které by sloužily k zachování kontinuity po ještě delší časové období, než jaké dokáže překlenout jedno časové razítko.

---

[6] Úroveň EPES přidává identifikátor SignaturePolicyIdentifier, pevně nastavený na svou implicitní hodnotu.

Filosofie implementace konceptu XAdES v MS Office 2010 je přitom taková, že uživatel si může nastavit dvě různé číselné hodnoty, v rozsahu 0 až 5 (ve smyslu výše uvedeného číslování úrovní XAdES):

- **XAdESLevel:** požadovaná úroveň XAdESpodpisu
- **MinXAdESLevel:** minimální přípustná úroveň XAdES podpisu

První z nich (XAdESLevel) říká, o jakou úroveň podpisu se má při vytváření usilovat. Pokud to nebude možné, může být vytvořen podpis na nižší úrovni, ale ta nesmí být nižší než druhá z hodnot (MinXAdESLevel).

> Například nastavení XAdESLevel=5 a MinXAdESLevel=2 znamená, že program vytvářející elektronický podpis se má snažit vytvořit podpis na úrovni XAdES-X-L (a tedy včetně časového razítka a revokačních informací). Pokud se mu to nedaří, může vytvořit i elektronický podpis na některé nižší úrovni, ale nejméně na úrovni XAdES-T (tedy s časovým razítkem).

Pro praxi jsou přitom nejužitečnější (a nejčastěji požadované) právě úrovně 2 (XAdES-T, s časovým razítkem) a 5 (XAdES-X-L, s časovým razítkem, nadřazenými certifikáty a revokačními informacemi přímo v dokumentu).

Úrovně 3 a 4 nejsou pro praxi tolik atraktivní proto, že u nich se revokační informace (nadřazené certifikáty a CRL seznamy či odpovědi OCSP serverů) uchovávají mimo samotný dokument. Jejich dostupnost v nějakém pozdějším okamžiku (při vyhodnocování podpisu) pak může být problematická.

Položky XAdESLevel a MinXAdESLevel je možné nastavit i na úroveň 0, která požaduje použití základního (a nerozšířeného) standardu XML-DSig pro ukládání elektronických podpisů do XML dokumentů. Takže například nastavení XAdESLevel=0 a MinXAdESLevel=0 zcela „vypíná“ XAdES podpisy. Ty jsou pak vytvářeny jen dle XML-DSig, kterému rozumí i programy z MS Office 2007 – bez časového razítka a revokačních informací.

Takovéto nastavení – které fakticky „vypíná“ XAdES – lze využít pro dosažení zpětné kompatibility s programy MS Office verze 2007.

Vedle toho ale existuje ještě jedna možnost, kterou je vytváření „zpětně kompatibilních“ XAdES podpisů (podrobněji viz část 7.3.4). Jejich princip je takový, že aplikace MS Office 2010 takovéto XAdES podpisy „vidí“ a pracují s nimi, zatímco aplikace MS Office 2007 je „nevidí“ a nepracují s nimi.

7.3.1.1 Nastavení XAdES

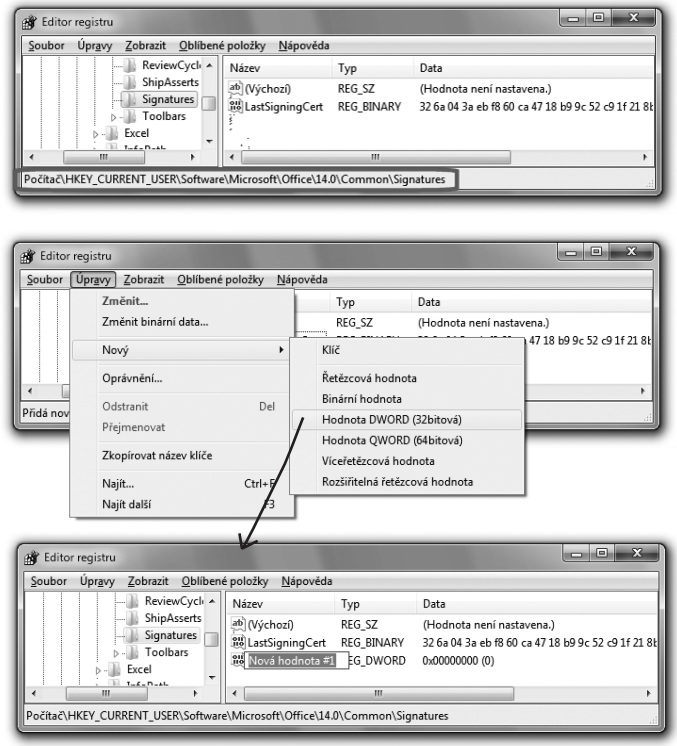
Nepříjemným problémem implementace XAdES podpisů v kancelářském balíku MS Office je nemožnost nastavit obě požadované hodnoty (**XAdESLevel** a **MinXAdESLevel**) nějakým uživatelsky vstřícným způsobem, přes uživatelské rozhraní příslušných programů (jako je MS Word) či jiné „uživatelské“ rozhraní.

Místo toho je pro jejich nastavení nutné využít pokročilých nástrojů pro správce, které ale nemusí být pro běžné uživatele k dispozici. Proto si zde ukážeme dosažení stejného efektu skrze přímý zásah do tzv. registru, byť určitě také nejde o řešení vhodné pro běžné uživatele. Ale je alespoň pro každého k dispozici, díky dostupnosti editoru registru (programu **regedit.exe**).

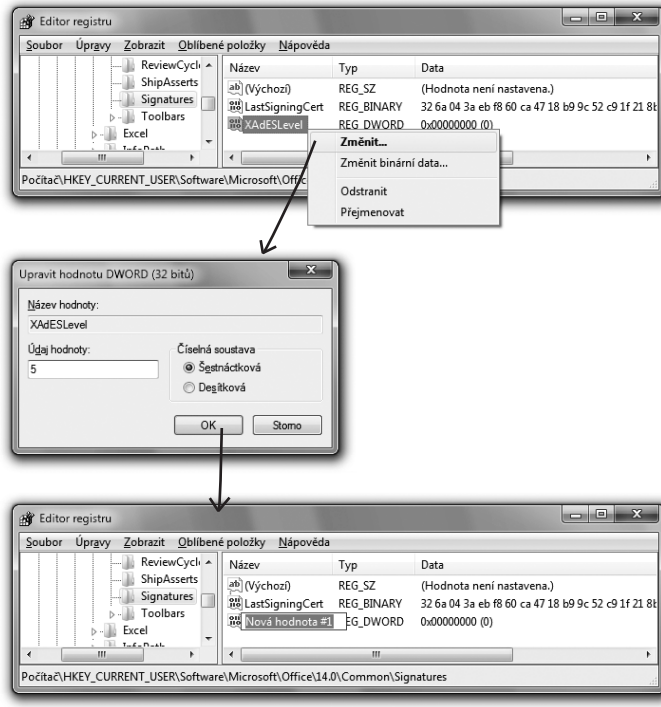
> Příslušné nastavení vyžaduje vytvořit tři nové položky v registru: dvě položky se musí jmenovat XAdESLevel a MinXAdESLevel, být typu REG-DWORD (jejich význam byl popsán výše). Třetí položka se musí jmenovat TSALocation, být typu REG-SZ a nabývat jako své hodnoty URL odkazu na server autority časového razítka, který poskytuje své služby dle RFC 3161 a na bázi HTTP protokolu. Příklad vytvoření příslušných položek, určený zkušenějším uživatelům, ukazují následující obrázky.

Obrázek 7-18

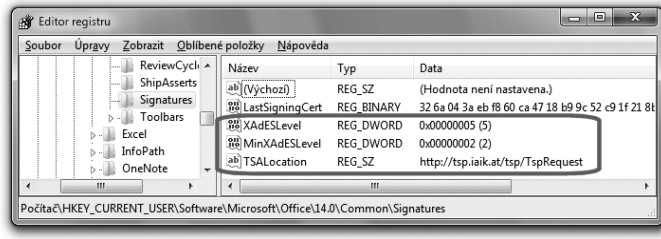
Vytvoření nové položky typu DWORD



Obrázek 7-19
Nastavení nové položky (XAdESLevel, na hodnotu 5)



Obrázek 7-20
Příklad celého nastavení pro XAdES



7.3.1.2 Vytváření neviditelných XAdES podpisů

XAdES podpisy mohou být v MS Office verze 2010 jak viditelné, tak i neviditelné. Zde si nejprve ukážeme pouze vytváření neviditelných XAdES podpisů.

Samotné vytváření (neviditelných) XAdES podpisů se v principu nijak neliší od vytváření jiných (ne-XAdES) elektronických podpisů. Tedy ani od vytváření „dřívějších“ XML-DSig podpisů, které používá verze MS Office 2007 (a které nemohou obsahovat ani časové razítko, ani revokační informace), a které dokáže vytvářet i MS Office 2010 (při nastavení položek XAdESLevel a MinXAdESLevel na hodnotu 0).

Konkrétní postup je obdobný tomu, který jsme si popisovali pro verzi 2007: jen přístup k nabídce vytvoření podpisu nevede přes „tlačítko Office“, ale přes nový **Backstage View**, dostupný pod záložkou **Soubor**.

Obrázek 7-21
Přístup k nabídce vložení elektronického podpisu v MS Word 2010 přes Backstage View

Zde již se nachází záložka **Informace**, a přes ni se lze dostat k nabídce **Zamknout dokument**. V ní se již nachází možnost připojení elektronického podpisu (prezentovaná ovšem jako možnost připojení podpisu digitálního).

Důležité přitom je, že uživatel zde již nemá žádnou možnost ovlivnit druh podpisu, který takto vznikne. To je v tuto chvíli pevně dáno nastavením položek XAdESLevel a MinXAdESLevel v registru, viz výše. Co uživatel změnit může, je certifikát, na kterém má být jeho podpis založen. Stejně tak může připojit jakýkoli text (fakticky: komentář) jako účel podepsání dokumentu, viz obrázek.

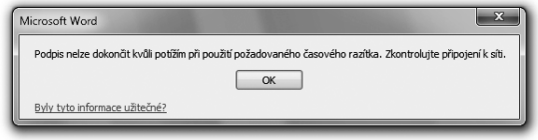
Obrázek 7-22
Okno pro podpis – s možností zadat účel a vybrat (změnit) certifikát

Vzhledem k nastavení položek XAdESLevel a MinXAdESLevel (které mohou být nastaveny na různé hodnoty) může vytvoření podpisu dopadnout různě – podle toho, zda jsou či nejsou k dispozici údaje, potřebné pro vytvoření vyšších úrovní podpisu.

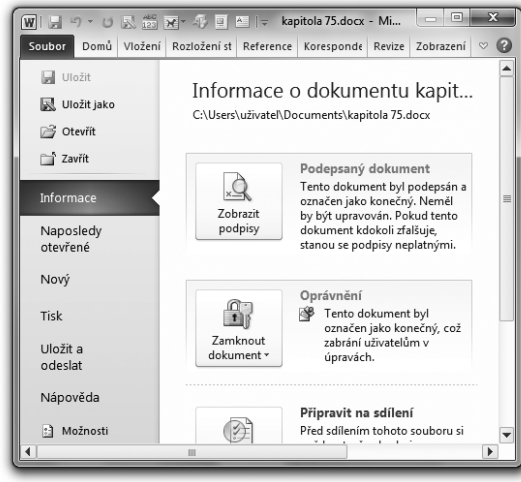
Uživatel se ale o výsledku (úrovni vytvořeného podpisu) v rámci samotného podepisování nedozví. S jedinou výjimkou, kterou je nemožnost vytvořit podpis v zadaných mezích (daných nastavením položek XAdESLevel a MinXAdESLevel).

Tato chybová situace je nejčastěji signalizována jako nemožnost získání časového razítka, kterou se MS Office snaží vysvětlit nemožností přístupu k síti.[7]

Obrázek 7-23
Hlášení o nemožnosti vytvořit časové razítko



Obrázek 7-24
Pohled Backstage View indikuje, že dokument je podepsán

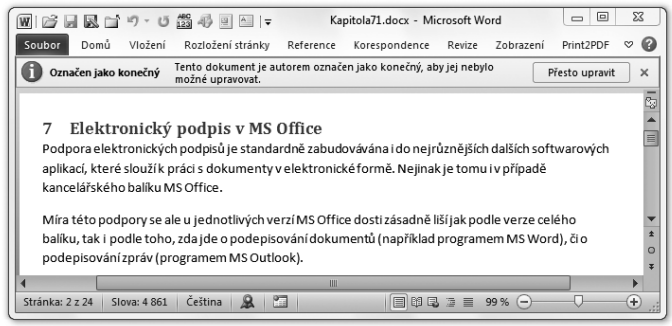


Pokud je požadovaný podpis úspěšně vytvořen, projeví se to ihned na pohledu Backstage View, viz spodní obrázek. Tento pohled také signalizuje, že dokument byl v důsledku svého podpisu uzamčen pro změny (a označen jako „konečný“).

Skutečnost, že dokument je podepsán, je pochopitelně signalizována i při běžném pohledu na právě otevřený dokument, skrze tradiční ikonku ve stylu červené pečeti (ve stavovém řádku).

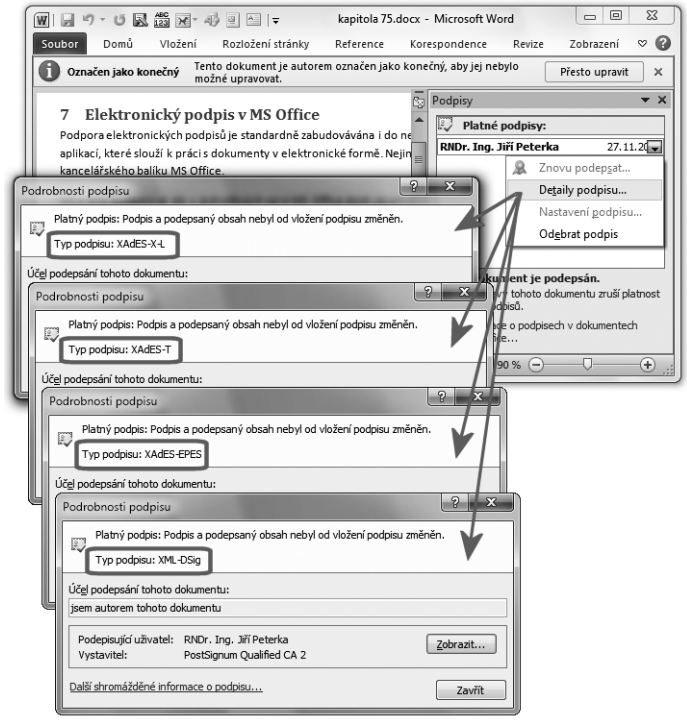
[7] Ta ale nemusí být skutečnou příčinou, zde znázorněný příklad je důsledkem uměle vytvořené chyby v URL odkazu na autoritu časového razítka.

Obrázek 7-25
Indikace, že právě otevřený dokument je elektronicky podepsán



Informaci o tom, jaký druh podpisu byl skutečně vytvořen, lze získat až při detailním pohledu na vlastnosti podpisu. Ten lze iniciovat jak z pohledu Backstage View, tak i poklepáním na ikonku ve tvaru pečeti, indikující přítomnost elektronického podpisu. V okně, které ukazuje výčet všech popisů na dokumentu a jejich platnost, je pak třeba si nechat zobrazit detaily podpisu, viz obrázek.

Obrázek 7-26
Detailní informace o podpisu, ze kterých již vyplývá i druh podpisu, včetně úrovně XAdES



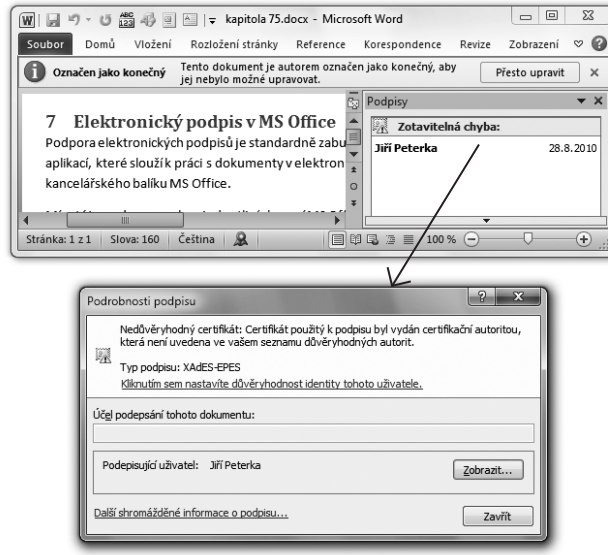
Pozor je třeba dávat na to, že nové nastavení položek registru (pro volbu úrovně XAdES podpisu, případně pro úplné „vypnutí“ XAdES) účinkuje až po restartu příslušné aplikace (např. MS Wordu), a nikoli ihned po samotné změně obsahu registru.

7.3.2 Ověřování podpisů

Způsob ověřování (vyhodnocování platnosti) elektronických podpisů na dokumentech v rámci balíku MS Office verze 2010 je v některých ohledech stejný jako u předchozí verze 2007.

Beze změny zůstává například to, že k vyhodnocování platnosti podpisů dochází automaticky při otevírání dokumentů příslušnou aplikací, a naopak jej není možné vyvolat někdy později, v době, kdy je dokument již otevřen. Výjimkou jsou pochopitelně nové, resp. právě vytvořené podpisy.

Beze změny je v nové verzi také to, že kontrolu revokace certifikátů ve skutečnosti zajišťuje operační systém, na kterém program Word 2010 běží – a tak se i u něj opakuje stejné chybné chování, popisované již v části 7.2.1 (kdy hodnotí platnost podpisu bez kontroly revokace, a uživatele o tom neinformuje). Výjimku by ale měly mít XAdES podpisy na úrovni X-L (eXtended Long term, neboli úrovně 5), které by si měly „nést přímo v sobě“ vše, co je k jejich ověření třeba, včetně revokačních informací.[8]



Obrázek 7-27
Příklad zotavitelné chyby (certifikát s vlastním podpisem není považován za důvěryhodný)

[8] Revokační informace jsou vkládány do podepisovaného dokumentu v okamžiku vzniku podpisu. Pokud se jedná o revokační informace získávané ze seznamů CRL, pak je nutné počítat s tím, že tyto seznamy jsou vydávány s určitým časovým zpožděním (až 24 hodin), a při následném ověřování proto není možné vystačit jen s obsahem těch verzí seznamů CRL, které byly k dispozici v okamžiku vzniku podpisu. Samotný standard XAdES řeší tento problém požadavkem na to, aby v případě CRL seznamů byly revokační informace připojovány k samotným podpisům až „někdy později“ (když už jsou k dispozici). Implementace XAdES v balíku MS Office 2010 podporuje jiné řešení: možnost omezit se jen na odpovědi OCSP serverů, které poskytují požadované informace v reálném čase. K aktivaci této možnosti je třeba nastavit v registru položku RequireOCSP na 1 (ve složce HKCU\software\microsoft\office\14.0\common\signatures pro Office 2010).

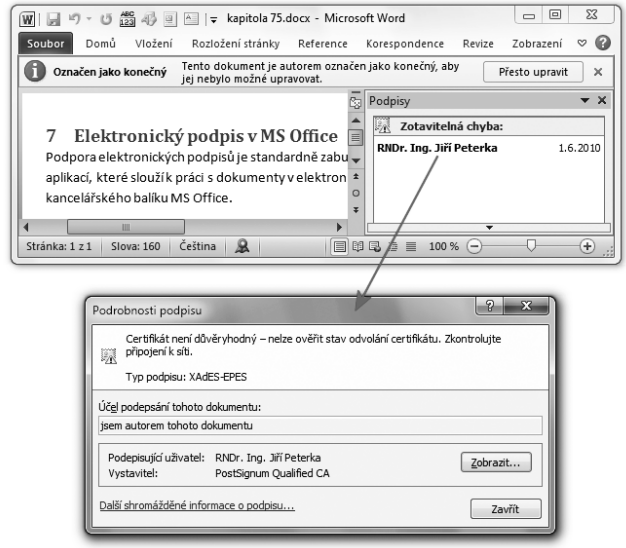
Odlišností od předchozí verze je pak vše, co souvisí s podporou XAdES podpisů: ve verzi Office 2010 musí být při ověřování vyhodnocováno všechno to, co je k samotným podpisům přidáváno v rámci příslušné úrovně XAdES.

Zajímavou odlišností oproti verzi 2007 je také rozlišování tří možných výsledků ověření (vyhodnocení platnosti) elektronického podpisu: ke dvěma možnostem (**platný** a **neplatný** podpis), se kterými pracovala verze 2007, nyní přibývá i třetí možný stav, a to **zotavitelná chyba** (anglicky **Recoverable Error**). Tak je v MS Office 2010 hodnocena situace, kdy určitým úkonem, resp. zásahem uživatele je ještě možné dosáhnout toho, že podpis může být považován za platný.

Příkladem může být situace z předchozího obrázku, kdy je podpis na dokumentu založen na certifikátu s vlastním podpisem (self-signed) – ale u tohoto certifikátu chybí důvod, díky kterému by mohl být považován za důvěryhodný (jeho přítomnost v příslušné složce právě používaného úložiště důvěryhodných certifikátů). Uživateli je zde nabízena možnost vyjádřit tomuto certifikátu důvěru jediným kliknutím (viz obrázek, odkaz „Kliknutím sem nastavíte důvěryhodnost identity tohoto uživatele“), a to dokonce bez povinného zobrazení příslušného certifikátu!

Jiným příkladem může být situace, kdy je podpis založen na takovém certifikátu, který není certifikátem s vlastním podpisem, ale pochází od „neznámého“ vydavatele. Přesněji: od takové certifikační autority, jejíž certifikát či certifikáty nejsou právě uloženy v příslušných složkách úložiště důvěryhodných certifikátů.

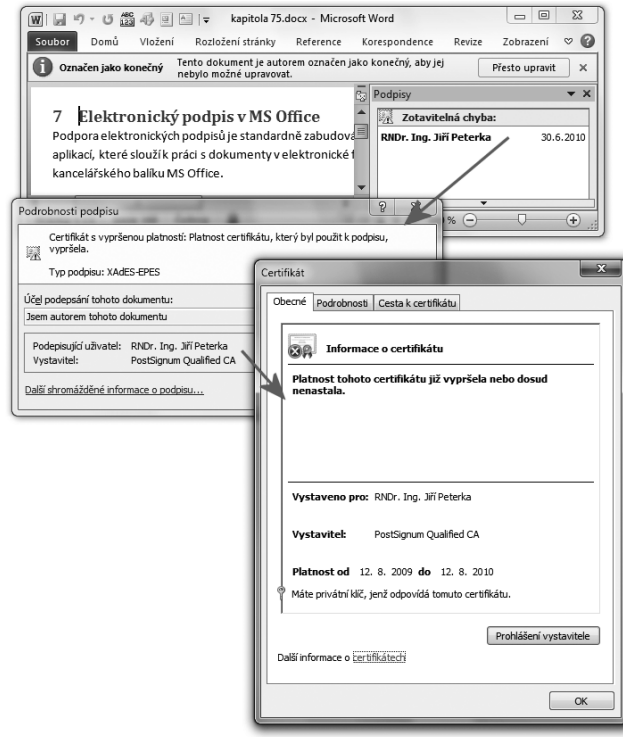
Obrázek 7-28
Příklad zotavitelné chyby (nadřazený certifikát není k dispozici v úložišti)



Úkonem, který takovouto „zotavitelnou chybu“ dokáže napravit, je uložení těchto certifikátů do příslušných složek úložiště. To již ale není tak jednoduché, a tak zde není uživateli nabízena takováto „náprava na jedno kliknutí“, viz předchozí obrázek.

Zajímavé přitom je, jak MS Word 2010 tuto situaci interpretuje: jako nemožnost ověřit stav odvolání (revokace) certifikátu.[9]

MS Word 2010 ovšem hodnotí jako „zotavitelnou chybu“ i takovou situaci, kdy k podpisu na dokumentu není připojeno časové razítko, a tento podpis je založen na certifikátu, kterému již skončila jeho řádná platnost (tedy když jde o XML-DSig podpis či XAdES-BES či EPES podpis). Zde je ovšem velmi těžké si představit korektní nápravnou akci, která by chybový stav dokázala napravit („zotavit se“ z něj).



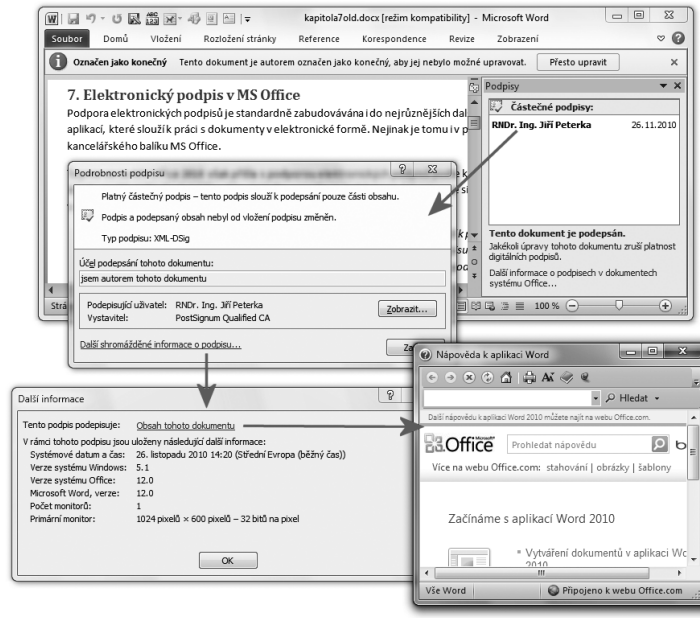
Obrázek 7-29
Příklad zotavitelné chyby (konec řádné platnosti certifikátu, absence časového razítka)

[9] Toto zřejmě souvisí s konkrétním postupem při vyhodnocování platnosti certifikátů v operačním systému MS Windows: ten vždy začíná na vrcholu certifikační cesty a nejprve se snaží ověřit případnou revokaci certifikátů bezprostředně pod kořenovým certifikátem. Když ale tento kořenový certifikát nemá k dispozici, nemůže ověřit podpis na revokačních informacích (seznamech CRL), a tak nemůže revokaci ověřit.

7.3.3 Částečné podpisy

V rámci kancelářského balíku MS Office 2010 zřejmě existuje ještě nejméně jeden podporovaný druh elektronického podpisu, a to „částečný“ podpis. Tedy takový, který podepisuje jen nějakou část dokumentu. V dostupné dokumentaci k MS Office 2010 ale o této možnost nejsou žádné další informace, kromě zmínky o tom, že „částečné podpisy“ je možné pouze vyhodnocovat (ověřovat), ale nikoli vytvářet.

Jak ukazuje i následující obrázek, práce s takovýmito částečnými podpisy je problematická i proto, že standardní cestou nejde zjistit, která část dokumentu je vlastně podepsána: příslušný odkaz (viz obrázek) vede jen na nápovědu k MS Office.



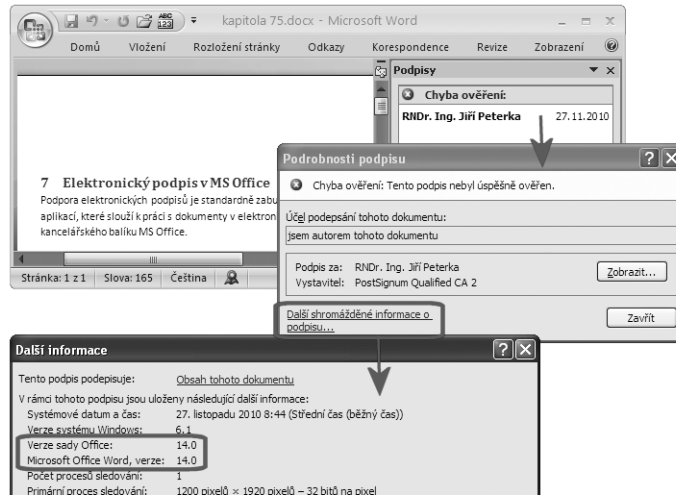
Obrázek 7-30
Částečný podpis v programu MS Word 2010

7.3.4 Zpětná kompatibilita XAdES podpisů

Vzhledem k tomu, že podpora konceptu XAdES byla zavedena až ve verzi MS Office 2010, není zajištěna zpětná kompatibilita XAdES podpisů s předchozími verzemi téhož balíku.

V praxi to znamená, že když je nějaký dokument opatřen XAdES podpisem v programu ve verzi 2010, je sice možné tento dokument přečíst ve stejném programu ve verzi 2007, ale příslušný podpis není možné ověřit. Uživatel přitom ale není informován o tom, že jde o nepodporovaný druh podpisu, který může být platný. Místo toho se dozví pouze to, že ověření podpisu se nezdařilo, viz následující obrázek.

Obrázek 7-31
Vyhodnocení platnosti XAdES podpisu z verze 2010 v MS Wordu verze 2007



Bohužel není k dispozici ani žádná detailnější indikace toho, o jakou chybu se jedná. Nepomůže ani zobrazení certifikátu, na kterém je podpis založen (ten může být zcela v pořádku – platný, nerevokovaný a důvěryhodný).

Jediným vodítkem tak může být informace o tom, že podpis vznikl v novější verzi programu, resp. kancelářského balíku. Tuto informaci najdeme (podle předchozího obrázku) po kliknutí na „další shromážděné informace o podpisu“ v okně o podrobnostech podpisu. Verzi programu a balíku Office, ve které podpis vznik, zde poznáte podle čísla této verze: MS Office 2007 je verzí číslo 12, a MS Office 2010 je verzí 14.[10]

Zpětná kompatibilita mezi verzemi 2010 (14) a 2007 (12) je možná při „vypnutí“ podpory konceptu XAdES, kdy jsou elektronické podpisy vytvářeny jen podle standardu XML-DSig, který podporuje i verze 2007. Tedy bez rozšíření dle konceptu XAdES.

> Vytváření takovýchto podpisů lze ve verzi 2010 dosáhnout nastavením položek XAdESLevel a MinXAdESLevel na hodnotu 0.

Další možností pak je takové nastavení programů MS Office verze 2010, které způsobuje, že vytvářené podpisy (na bázi XML-DSig) sice obsahují rozšíření dle XAdES, ale starší programy (verze 2007) toto rozšíření dokáží ignorovat a nevšímat si ho.[11] Díky tomu dokáží starší programy pracovat alespoň se „základní částí“ podpisu dle XML-DSig, zatímco ty novější dokáží pracovat i s rozšířením XAdES.

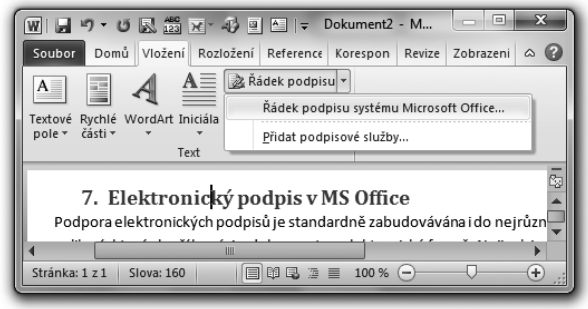
[10] Verze číslo 13 byla záměrně vynechána, prý kvůli negativním konotacím kolem čísla 13.

[11] Pro aktivaci této možnosti je třeba vytvořit v registru novou položku O12CompatibleXAdES ve složce HKCU\software\microsoft\office\14.0\common\signatures a nastavit ji na hodnotu 1.

7.3.5 Viditelné elektronické podpisy

Jak jsme si již uvedli, již ve verzi MS Office 2007 byla poprvé zavedena podpora viditelných podpisů, v obdobném smyslu jako například u PDF dokumentů. Tedy v takové podobě, která je „vidět“ na samotném dokumentu, ať již při jeho prohlížení pomocí příslušného programu, nebo po jeho vytištění. V MS Office 2010 pak byly i tyto viditelné podpisy obohaceny o podporu XAdES, ve stejném rozsahu jako podpisy neviditelné.

Obrázek 7-32
Vložení řádku podpisu do právě otevřeného dokumentu



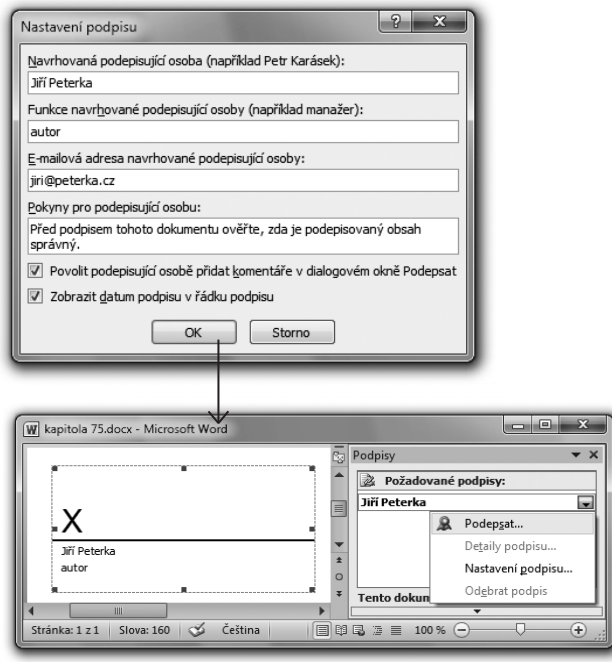
Princip práce s viditelnými podpisy v MS Office 2010 je podobný tomu, jak vše funguje u produktů společnosti Adobe (Acrobat a Reader) s „prázdnými podpisy“: nejprve se vytvoří, určitým způsobem předvyplní a do dokumentu umístí jakási šablona budoucího elektronického podpisu – v terminologii MS Office označovaná jako „**řádek podpisu**“. A ten se pak (kdykoli později) podepíše.

Řádek podpisu přitom může podepsat sám ten, kdo jej vytvořil a umístil do dokumentu – a to je pro něj vlastně i jediný možný způsob, jak do dokumentu přidat vlastní viditelný podpis. Stejně tak ale může řádek podpisu vytvořit a umístit do dokumentu jeho autor, s tím že podepisovat jej bude již někdo jiný (například nadřízený autora).

Zřejmě právě kvůli rozdělení rolí (autora dokumentu a podepisujícího) je možné do řádku podpisu předvyplnit řadu údajů, z nichž některé slouží spíše jako vzkaz pro budoucího podepisujícího, ve formě pokynů. Nechybí ani možnost uvést v řádku podpisu jméno a funkci (i e-mail) toho, kdo má dokument podepsat.

Výčet toho, co vše se dá do „řádku podpisu“ předvyplnit, ukazuje prostřední obrázek s oknem **Nastavení podpisu**.

Samotný řádek podpisu je pak objektem, který je vkládán do dokumentu na místo kurzoru. Lze jej různě zvětšovat a zmenšovat, posouvat či formátovat. Dokud je řádek podpisu nepodepsaný, je možné jej dokonce kopírovat na jiná místa v témže dokumentu či do jiných dokumentů. A každé umístění tohoto objektu v dokumentu mu přidává jeden „požadovaný podpis“, který se objevuje i v přehledu v okně podpisů, viz následující obrázek.



Obrázek 7-33
Předvyplnění „řádku podpisu“ a jeho umístění v dokumentu

V jednom dokumentu tedy může být i více „řádků podpisu“, které mohou být samostatně podepisovány.

Samotné podepsání předem připraveného „řádku podpisu“ je pak obdobné jako u neviditelného podpisu. Lze jej iniciovat například poklepáním na samotný objekt s řádkem podpisu, nebo skrze nabídku v okně s přehledem podpisů.

V rámci podepisování samozřejmě lze zvolit certifikát, na kterém má být podpis založen. Lze také zadat důvod podpisu, a do „řádku“ (u písmene X) lze znovu napsat vlastní jméno, nebo místo něj připojit fotografii.

Připomeňme si, že viditelný podpis, stejně jako podpis neviditelný, je u verze MS Office 2010 založen na rozšíření XAdES, a jeho vytváření se řídí stejnými pravidly (nastavením položek XAdESLevel a MinXAdESLevel v registru, viz výše).

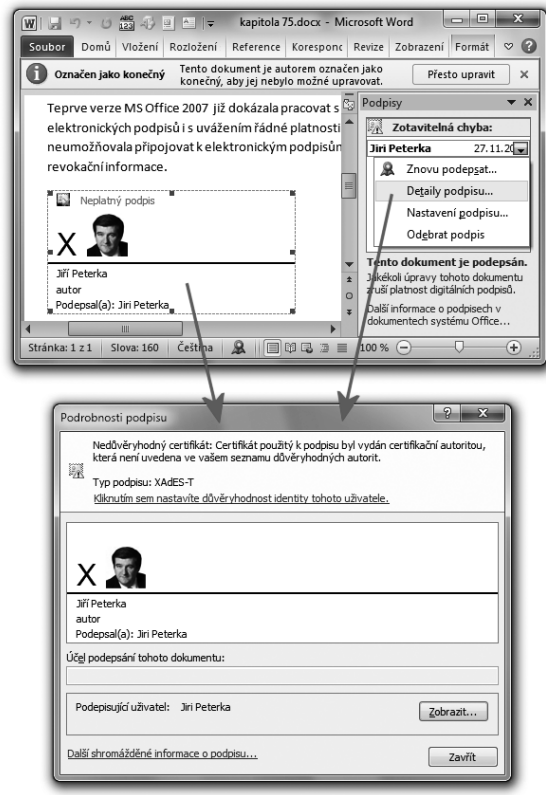
Viditelný podpis (včetně XAdES) je v rámci balíku MS Office dostupný v programech Word, Excel a InfoPath. Není dostupný v programu PowerPoint, který podporuje pouze neviditelné podpisy.

Pokud jde o ověřování viditelných podpisů, i to se řídí úplně stejnými pravidly jako u podpisů neviditelných. Jedinou odlišností tak může být indikace stavu, kdy viditelný podpis není hodnocen jako platný – tato skutečnost je zobrazována přímo v rámci viditelného podpisu.

Obrázek 7-34

Příklad práce s „řádky podpisu“

Obrázek 7-35
Důvod neplatnosti podpisu v podpisovém řádku



Jak ale ukazuje příklad na předchozím obrázku, toto hodnocení nemusí být konzistentní: na samotném viditelném podpisu je podpis hodnocen jako neplatný, zatímco v okně pro podpisy je hodnocen jako podpis se zotavitelnou chybou, kterou lze napravit.

7.4 Elektronické podepisování e-mailových zpráv

Možnost přidávat elektronický podpis ke zprávám elektronické pošty (neboli: podepisovat je), se v rámci kancelářského balíku MS Office objevuje dokonce ještě dříve, než možnost podepisování dokumentů: program MS Outlook měl tuto schopnost již v rámci MS Office verze 98 (zatímco možnost podepisování dokumentů se objevuje až ve verzi 2002/XP).

Připomeňme si, že u e-mailových zpráv se lze setkat také s „textovými podpisy" ve formě patiček, které se automaticky vkládají obvykle na konec zprávy, ale plní pouze informační funkci (viz část 4.1). Těmito podpisy, které nemají charakter zaručeného elektronického podpisu, se zde zabývat nebudeme.

Stejně tak si hned v úvodu zdůrazněme, že podpora podepisování e-mailových zpráv je v rámci balíku MS Office od začátku řešena samostatně a nezávisle na možnosti podepisování dokumentů. Důvodem je nejspíše skutečnost, že konkrétní způsob vkládání (interních) elektronických podpisů do e-mailových zpráv a do dokumentů se zásadně liší.

> Připomeňme si, že pro vkládání podpisů do dokumentů používaly první verze MS Office (2002/XP a 2003) vlastní specifický formát. Teprve verze 2007 přešla na používání standardu XML-DSig, a verze 2010 jej rozšířila o podporu XAdES podpisů.

Naproti tomu pro podepisování e-mailových zpráv, resp. k začleňování podpisů do zpráv, se dnes využívá standard S/MIME. Ten byl poprvé implementován v Outlooku 98 (ve verzi S/MIME 2), a již Outlook 2000 podporoval stejnou verzi S/MIME 3, s jakou pracují i nejnovější verze tohoto programu.

To, co naopak mají obě varianty podepisování (dokumentů a zpráv) v rámci MS Office všech verzí společné, je využití prostředků a služeb systémového úložiště v MS Windows pro práci s certifikáty a jejich vyhodnocování. Jinými slovy: jak MS Word, Excel a PowerPoint či InfoPath, tak i Outlook si nechávají vyhodnocovat certifikáty od operačního systému Windows, skrze jeho služby.

Výhodou je „společný efekt“ systémového úložiště: je-li nějaký certifikát považován za důvěryhodný díky svému uložení v systémovém úložišti důvěryhodných certifikátů, bude důvěryhodný jak pro Outlook (pro podpisy na zprávách), tak i pro Word, Excel a další (pro podpisy na dokumentech).

Nevýhodou je naopak to, že chybné postupy při vyhodnocování certifikátů se promítají stejným způsobem jak do ověřování podpisů na dokumentech (viz část 7.2.1.), tak i do ověřování podpisů na zprávách.

7.4.1 Profily (nastavení zabezpečení)

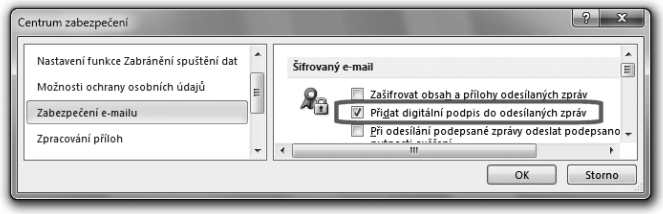
Zajímavou odlišností (od podepisování dokumentů) je již samotný výběr certifikátu, na kterém má být podpis založen.

Při podepisování dokumentů je uživateli pokaždé (při každém jednotlivém podpisu) nabídnuta možnost určit certifikát, na kterém má být podpis založen. Přesněji: jeden je přednastavený a uživatel má možnost jej změnit. Navíc má možnost připsat ještě komentář, jako „důvod podpisu“.

Při podepisování zpráv (v MS Outlooku) ale uživatel takovouto možnost nemá – ani nemůže připsat účel podpisu, ani nemůže vybrat ten certifikát, na kterém má být podpis založen.

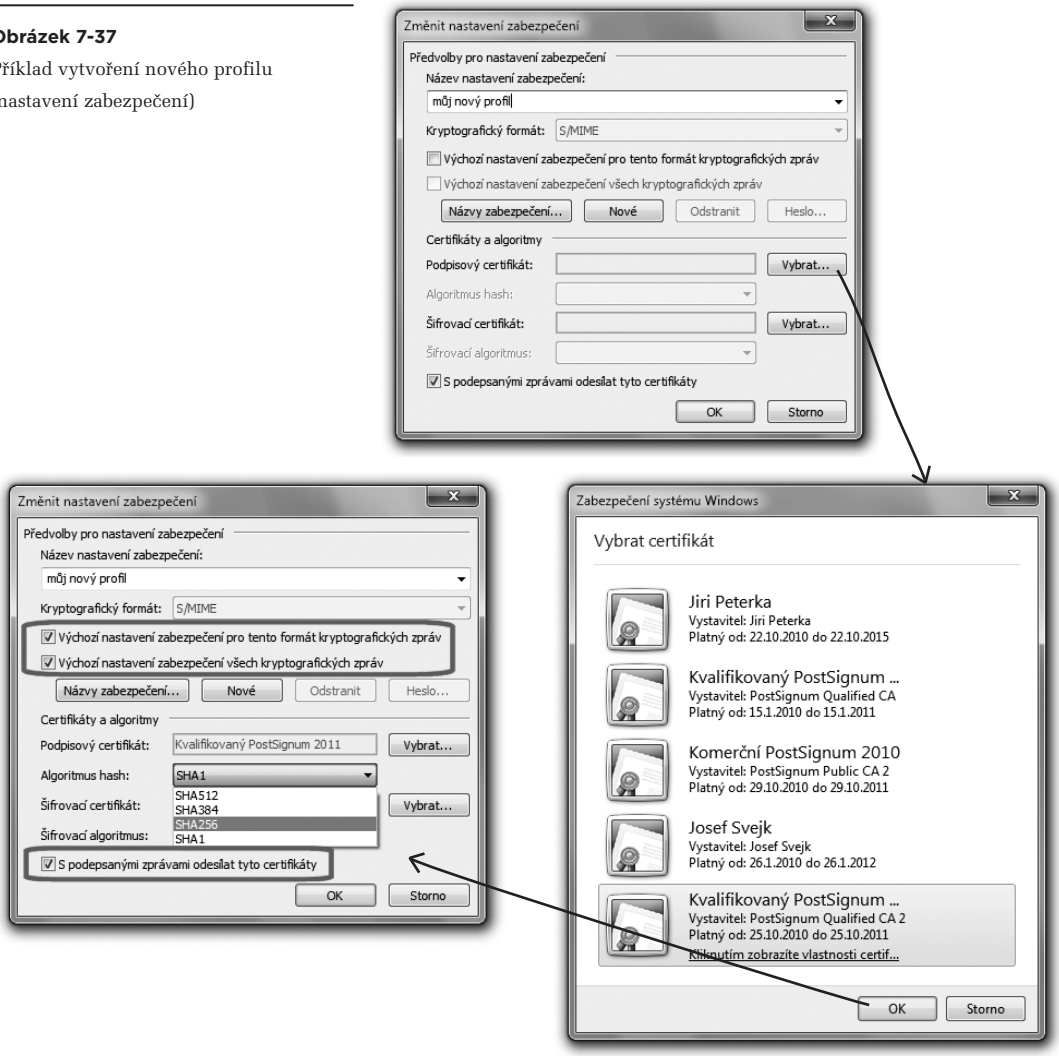
Zde vše funguje na jiném principu: místo volby „v okamžiku podpisu“ má uživatel možnost si dopředu připravit několik „podpisových profilů“, a jeden z nich prohlásit za výchozí. Podle něj pak bude každý jednotlivý podpis na zprávě vytvořen, do příští změny výchozího profilu.

Obrázek 7-36
Možnost nastavit automatické podepisování všech odesílaných zpráv



Důvodem pro volbu takovéhoto řešení může být to, že k podepisování zpráv nemusí docházet jen na explicitní pokyn uživatele, ale může se tak dít i automaticky, na základě „trvalé“ předvolby, viz obrázek.

Obrázek 7-37
Příklad vytvoření nového profilu (nastavení zabezpečení)



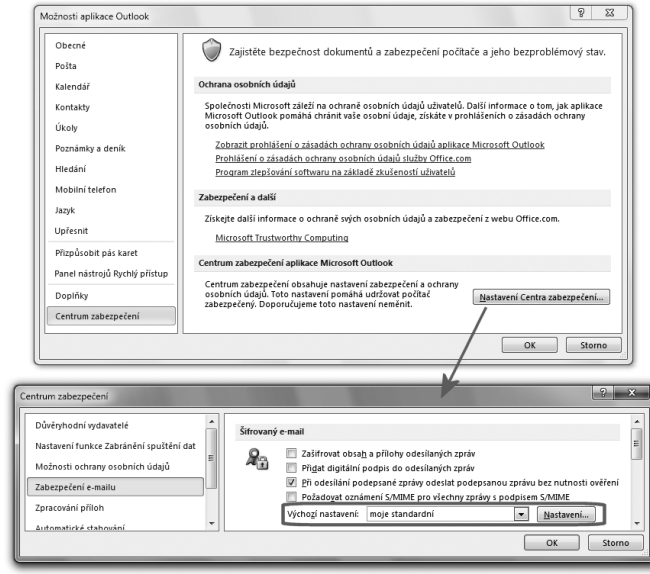
Příslušný „profil“ je v terminologii MS Office označován jako „nastavení zabezpečení“, kvůli tomu že zahrnuje i nastavení týkající se šifrování (viz část 8.1.3). Pro potřeby podepisování se v něm vybírá ten certifikát, na kterém mají být založeny následně vytvářené podpisy.

Stejně tak lze nastavit i algoritmus otisku (v rámci možností daných certifikátem) – což u podepisování dokumentů je možné jen skrze nastavení registru.

Současně se na profilu dá nastavit i to, zda právě on má být tím aktuálním, který bude automaticky použit při vytváření každého dalšího podpisu (viz volba „výchozí nastavení“ na předchozím obrázku).

V neposlední řadě lze již v rámci profilu (formálně: „nastavení zabezpečení“) specifikovat i to, zda má být k odesílaným podepsaným zprávám připojen i samotný podpisový certifikát, a stejně tak i certifikát šifrovací. Kladné nastavení (zaškrtnutí) zde lze jen doporučit, resp. mělo by být standardem: přiložení podpisového certifikátu usnadňuje práci příjemci, který pak nemusí složitě shánět certifikát podepsané osoby, který potřebuje pro ověření podpisu, ale najde jej rovnou v samotné zprávě. A jak uvidíme v části 8.1.3, náš šifrovací certifikát potřebuje příjemce zase k tomu, aby (tímto certifikátem) mohl zašifrovat svou odpověď, určenou jen a jen pro nás.

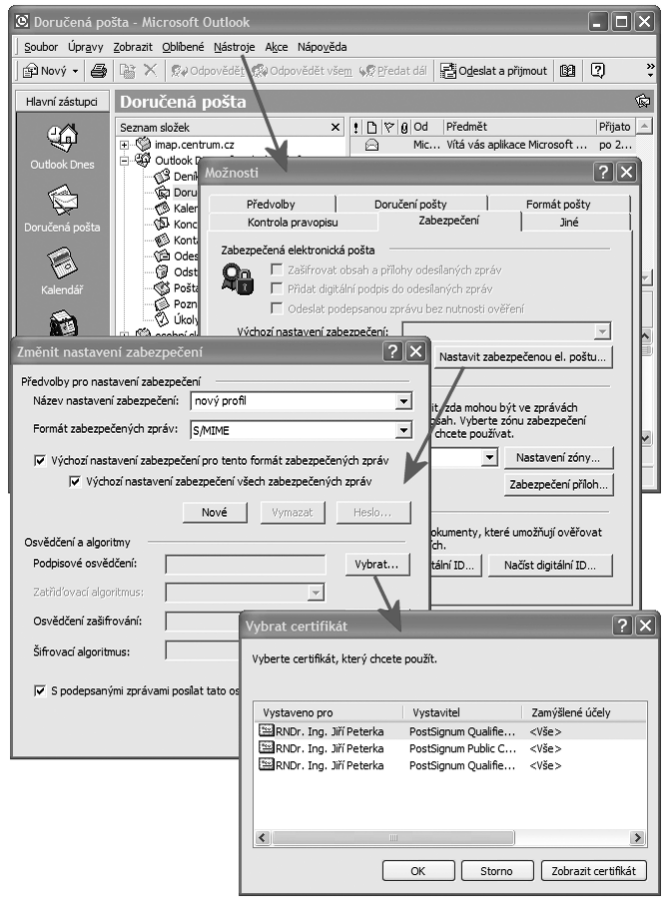
Možnost volby profilu (nastavení zabezpečení) či vytvoření nového profilu jsou v novějších verzích programu Outlook (2007 a 2010) dostupné přes **Možnosti aplikace Outlook**, ke kterým se lze dostat buďto přes „tlačítko Office“ (u verze 2007) nebo přes **Backstage View** (u verze 2010). Dále je třeba pokračovat přes volbu **Centrum zabezpečení**, tlačítko **Nastavení Centra zabezpečení**, a dále přes volbu **Zabezpečení e-mailu**.



Obrázek 7-38
Dostupnost nabídky změny profilu a vytvoření nového (MS Outlook 2007 a 2010)

U starších verzí MS Outlook je stejná možnost dostupná přes položku **Nástroje** v hlavním menu, dále volbu **Možnosti** a pak dle následujícího obrázku. Povšimněte si na něm ještě staršího pojmu „osvědčení“, používaného místo dnes běžného pojmu „certifikát“.

Obrázek 7-39
Dostupnost nabídky změny profilu či vytvoření nového (MS Outlook 2000)

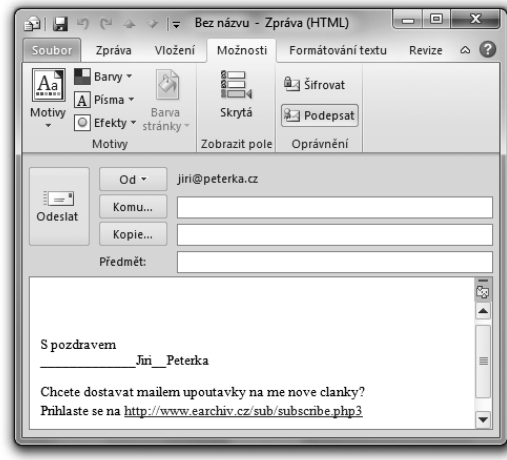


7.4.2 Podepisování odesílaných zpráv

Podepisování odesílaných zpráv, poté co je nastaven a zvolen výchozí profil, je již velmi jednoduché. O tom, zda podpis bude či nebude k odesílané zprávě skutečně připojen (resp. zpráva podepsána), samozřejmě rozhoduje vždy uživatel, prostřednictvím ikony (**Podepsat**) v menu.

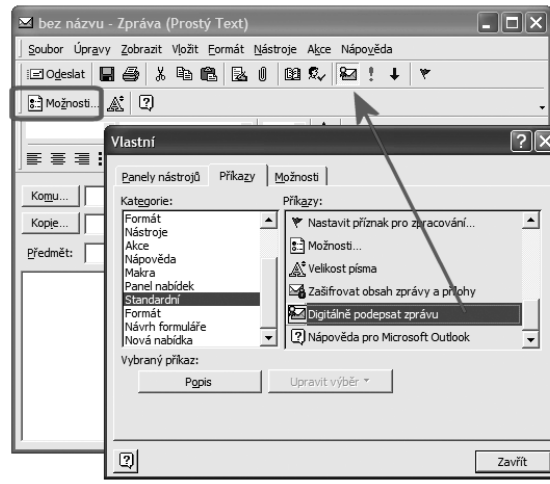
Tuto ikonu lze u MS Outlooku 2010 nalézt na kartě Možnosti, ve skupině Oprávnění, viz obrázek.

Obrázek 7-40
Volba pro podepsání nové zprávy (MS Outlook 2010)



Volba ve výchozím profilu („Přidat digitální podpis do odesílaných zpráv“) přitom funguje jako předvolba této ikonky: pokud je volba v profilu aktivní (zaškrtnutá), pak je aktivní (navolená) i ikonka požadující podpis dané zprávy. Uživatel ale může tuto volbu u každé zprávy libovolně měnit, klikáním na ikonku. Ovšem pokud tak neudělá, například pokud se na kartu „Možnosti“ vůbec nepodívá, a pokud je předvolba aktivní, jsou všechny odesílané zprávy automaticky podepisovány (a uživatel si toho ani nemusí být vědom).

Obrázek 7-41
Úprava menu, aby obsahovalo ikonku pro podepsání odesílané zprávy



U Outlooku 2007 je ikonka pro podepsání nové zprávy standardně umístěna již na kartě „Zpráva“. Obdobně pro přeposílané zprávy a odpovědi na došlé zprávy.

U starších verzí MS Outlook ale není ikonka pro podepsání zprávy standardně dostupná a musí se do menu nejprve přidat. Nebo je nutné u každé odesílané zprávy využít nabídku „Možnosti“, ve které již je možné si vyžádat podepsání odesílané zprávy.

7.4.2.1 Význam podpisu na odesílané poštovní zprávě

V souvislosti s podepisováním odesílaných zpráv bychom měli mít na paměti, že připojovaný podpis „pokrývá“ (podepisuje) vždy celou zprávu, včetně případných příloh. Minimálně ve smyslu zajištění integrity: pokud by se něco změnilo buď na těle zprávy či na některé její příloze, došlo by k porušení integrity a elektronický podpis by se kvůli tomu stal neplatným.

Zajímavým rozdílem mezi podepisováním odesílaných zpráv a podepisováním dokumentů je pak to, že u zpráv nemáme možnost připojit ke svému podpisu nějaký komentář, v roli účelu podpisu. Jakoby se tím naznačovalo to, že účel podpisu je zde pevně dán, a to ve smyslu „*jsem odesilatelem této zprávy*“. Chápat tento účel ve smyslu „autorství“ lze asi jen na to, co má charakter sdělení v samotném těle zprávy (a co by ve světě listovní pošty odpovídalo průvodnímu dopisu). Již se ale nedá vztáhnout na přílohy: podpis celé e-mailové zprávy, do které jsou vloženy nějaké přílohy, rozhodně není možné automaticky chápat ve smyslu „*jsem autorem těchto příloh*“.

Vůči přílohám by význam podpisu na zprávě (jako celku) měl být chápán ve smyslu: „*jsem ten, kdo vložil tyto přílohy*“. Podpis pak stvrzuje to, že se přílohy během přenosu nezměnily (neporušila se jejich integrita).

> Jde o obdobnou situaci, jako u služby messengera, kterému předáte k transportu vámi napsaný dokument. Messenger jej vloží do přepravní obálky (která je analogií e-mailové zprávy) a tuto podepíše a doručí. Příjemce převezme přepravní obálku a z neporušeného podpisu messengera na obálce si může domyslet, že přeprava proběhla korektně a žádný z dokumentů v přepravní obálce nebyl pozměněn ani ztracen. Ze stejného podpisu si již ale rozhodně nebude domýšlet, že autorem dokumentu v přepravní obálce je sám messenger.

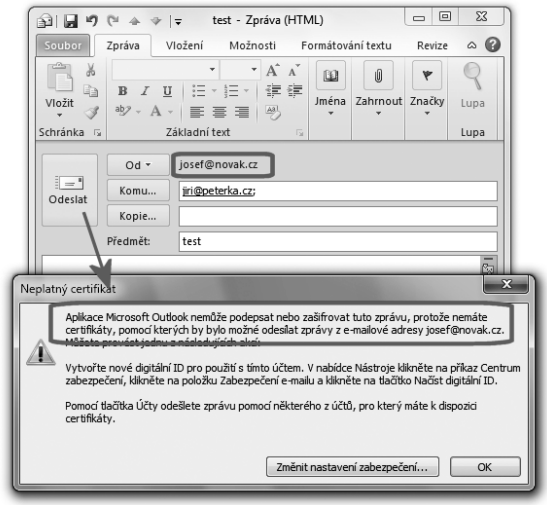
7.4.2.2 E-mailová adresa v certifikátu

Dalším praktickým aspektem, který se týká podepisování odesílaných zpráv, je nutnost shody mezi adresou odesilatele a e-mailovou adresou, uvedenou přímo v certifikátu.

Poštovní programy, včetně MS Outlooku, kontrolují shodu obou adres a bez ní nedovolí zprávu odeslat.

Fakticky to také znamená, že pokud chcete nějaký certifikát používat pro podepisování e-mailů, musíte již při žádosti o jeho vystavení pamatovat na to, že v něm musí být uvedena ta e-mailová adresa, ze které budete své maily odesílat.

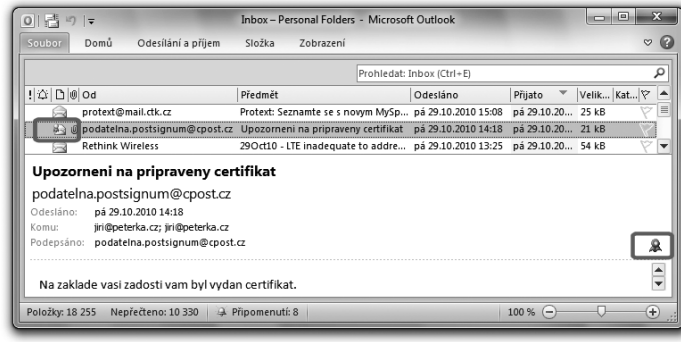
Obrázek 7-42
Při neshodě adres Outlook odesílanou zprávu nepodepíše



7.4.3 Příjem podepsaných zpráv

To, že konkrétní přijatá zpráva je podepsaná, lze poznat nejsnáze podle tradiční červené ikonky, stylizované do tvaru pečeti, viz obrázek.

Obrázek 7-43
Indikace podepsané zprávy v přehledu došlých zpráv

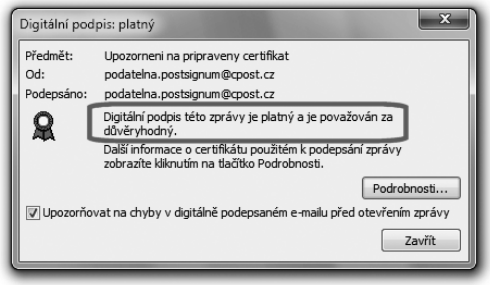


Poklepáním na tuto ikonku si lze vyžádat základní informaci o platnosti podpisu na zprávě. Samotný obsah zprávy se přitom zobrazí (v okně pro čtení či v samostatném okně s touto zprávou) pouze v případě, kdy je podpis k aktuálnímu okamžiku hodnocen jako platný.

V opačném případě (pokud není podpis na zprávě vyhodnocen jako platný) není obsah zprávy automaticky zobrazen.

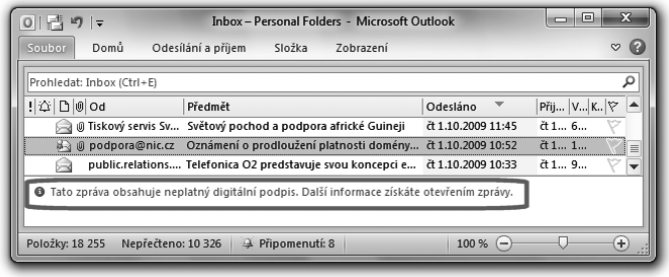
Obrázek 7-44

Informace o platnosti podpisu na zprávě



Obrázek 7-45

Není-li podpis na zprávě platný, není zpráva zobrazena



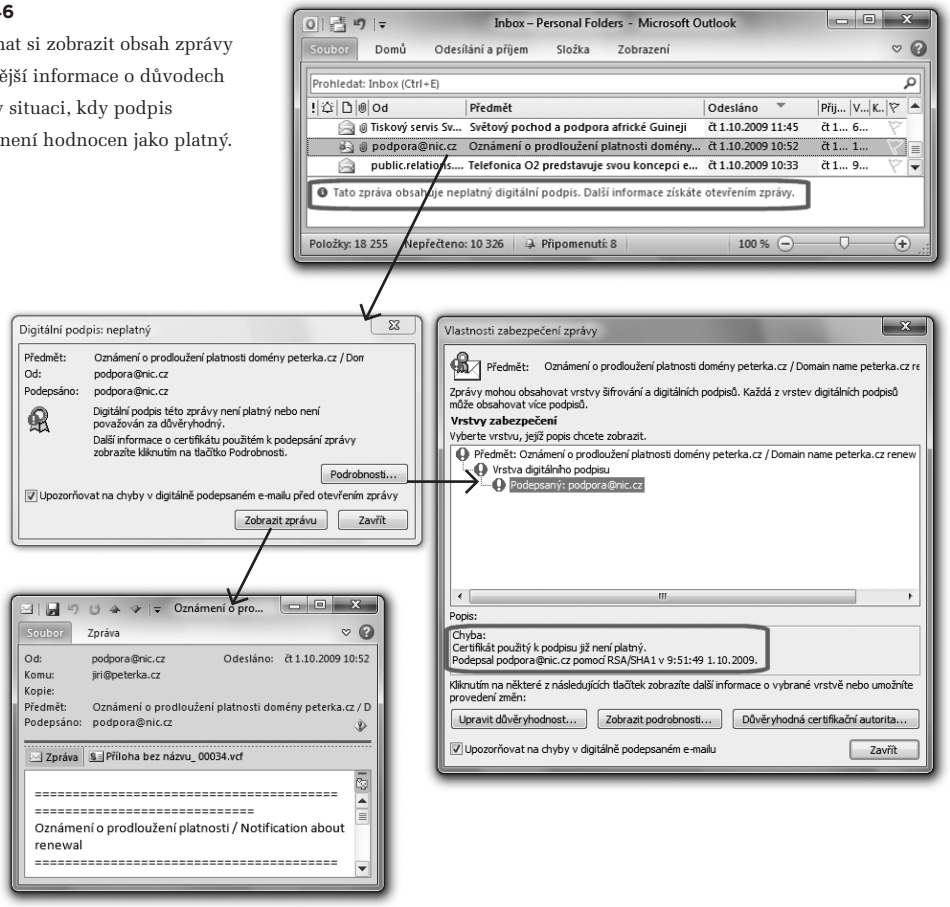
Zdůrazněme si, že MS Outlook (ani ve verzi 2010) nedokáže pracovat s časovými razítky. Proto jsou všechny podpisy na zprávách ověřovány k aktuálnímu časovému okamžiku.[12] Je tedy zcela běžné, že došlou zprávu lze po jejím doručení bez problémů zobrazit zcela standardním způsobem (jelikož její podpis je ještě považován za platný), ale později – po skončení řádné platnosti certifikátu, na kterém je podpis zprávy založen – již tomu může být jinak.

V době, kdy podpis na zprávě již není hodnocen jako platný, vede pokus otevřít zprávu (například poklepáním na řádek se zprávou v přehledu zpráv) pouze k otevření okna, které informuje o neplatnosti podpisu. I pak je ale možné se k obsahu zprávy dostat, protože toto okno již nabízí možnost zobrazit obsah zprávy (s upozorněním na neplatnost podpisu). Stejně tak nabízí možnost nechat si zobrazit podrobnosti o důvodech neplatnosti podpisu na zprávě.

V praxi může ověřování podpisů na přijímaných zprávách ovlivnit také antivirový program, pokud do zprávy přidá svou poznámku o provedené antivirové kontrole. Pokud tak učiní, poruší tím integritu již podepsané zprávy (změní její obsah) a způsobí tím neplatnost jejího podpisu.

12 I v souladu s pravidly pro ověřování, popisovanými v kapitole 3.

Obrázek 7-46
Možnost nechat si zobrazit obsah zprávy (nebo detailnější informace o důvodech neplatnosti) v situaci, kdy podpis na zprávě již není hodnocen jako platný.



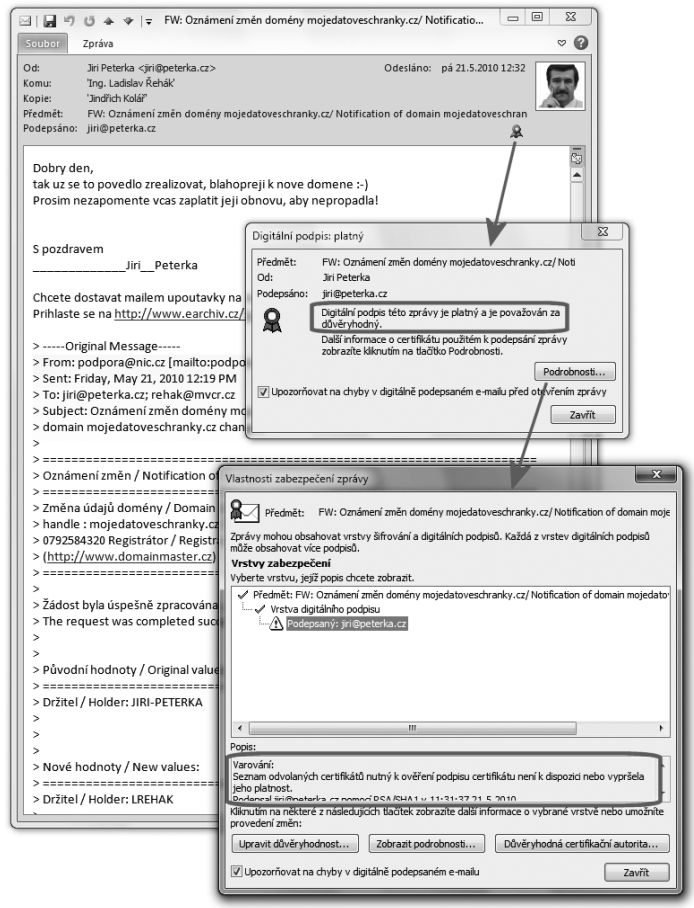
7.4.4 Ověřování podpisů v MS Outlook

Pro správné porozumění tomu, jak MS Outlook pracuje s elektronickými podpisy, si ještě musíme upřesnit, jakým způsobem je ověřuje, resp. jak vyhodnocuje jejich platnost.

V zásadě postupuje stejně, jako ostatní programy z balíku MS Office, a to verze 2007 – když rozeznává jen dva možné stavy, resp. výsledky vyhodnocení podpisu: platný a neplatný podpis.

Podobnost s ostatními programy je bohužel i v tom, že dělá stejné chyby, konkrétně při zjišťování stavu revokace právě posuzovaného certifikátu: příslušné informace si zjišťuje pouze tehdy, pokud má přístup on-line. Jinak nikoli – a pak se chová, jako kdyby certifikát nebyl revokovaný.

Obrázek 7-47
Příklad, kdy Outlook hodnotí podpis jako platný, i když neměl možnost ověřit případnou revokaci.

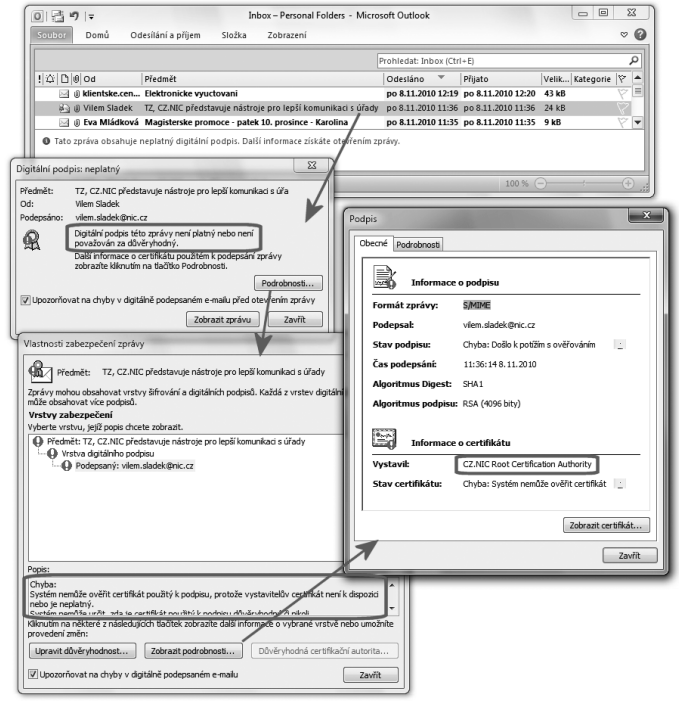


Uživateli to ale Outlook sám najevo nedá. Teprve pokud si uživatel nechá zobrazit podrobnosti o platně ověřeném podpisu, může se dozvědět, že toto ověření nebralo v úvahu případnou revokaci, protože potřebné informace nebyly k dispozici (viz předchozí obrázek).[13]

Jiným příkladem může být situace, kdy při ověřování podpisu není k dispozici některý z nadřazených certifikátů toho certifikátu, na kterém je podpis zprávy založen. Obvykle jde o certifikát vydavatele tohoto certifikátu (příslušné certifikační autority). Zatímco například Word 2010 by ve stejné situaci hodnotil vše jako „zotavitelnou chybu“ (viz část 7.3.2), Outlook 2010 to hodnotí rovnou jako neplatný podpis.

[13] Toto chování MS Outlooku lze ovlivnit nastavením položky UseCRLChasing v registru, ve složce HKCU\software\policies\microsoft\office\14.0\outlook\security: Standardně je nastavena na hodnotu 1, kdy se chová tak jak je popisováno (CRL seznam stahuje, jen když je online). Při nastavení na hodnotu 2 CRL seznam nestahuje vůbec, a pro UseCRLChasing=0 se chová dle implicitního nastavení systému.

Obrázek 7-48
Situace, kdy certifikát vydavatele není v úložišti důvěryhodných certifikátů, a Outlook vyhodnotil podpis jako neplatný.



7.5 MS Office a SHA-2

Na závěr této kapitoly, věnované problematice elektronického podpisu v kancelářském balíku MS Office, si ještě řekněme, jak je to s podporou hašovací funkce SHA-2.

> V souvislosti s tím si můžeme připomenout, že tuzemské certifikační autority smějí vydávat (od 1. 1. 2010) již jen takové certifikáty, které podporují SHA-2. Přesněji: které jsou samy vydány s využitím hašovací funkce SHA-2 (a klíčů o velikosti nejméně 2048 bitů).

Stejně tak si ale připomeňme, že povinnost používání SHA-2 se týká vydávání nových certifikátů, ale nikoli jejich používání širší uživatelskou veřejností. Vůči ní jde pouze o doporučení, ale nikoli o formálně závaznou povinnost.

Připomenout si můžeme i to, že „nové“ certifikáty (vydané již na bázi SHA-2) lze stále používat i „postaru“, neboli k vytváření takových elektronických podpisů, které využívají ještě původní hašovací funkci SHA-1.[14]

[14] Platí to dokonce i obráceně: „starý“ certifikát, vydaný ještě s SHA-1, lze využít k podepisování s SHA-2.

> O tom, zda je podpis na bázi SHA-1 stále přípustný, nebo nikoli (a zda je vyžadován podpis využívající již hašovací funkci SHA-2), pak obecně rozhoduje příjemce. V oblasti veřejné moci tedy ta konkrétní agenda, která elektronicky podepsané dokumenty přijímá.

Například Celní správa pro své agendy požaduje podpisy na bázi SHA-2 počínaje 1. 12. 2010.

Pokud jde o samotnou podporu hašovací funkce SHA-2 v jakýchkoli softwarových produktech – a nikoli pouze v těch od Microsoftu – pak je nutné mít na paměti, že tuto hašovací funkci musí podporovat celý řetězec prvků, který se na tvorbě podpisu či jeho ověření podílí. Tedy jak samotné aplikace, tak i operační systém, používané úložiště důvěryhodných certifikátů a také moduly CSP, které jsou využívány. Jakmile kterýkoli z prvků v tomto řetězci SHA-2 nepodporuje, není možné s touto hašovací funkcí pracovat.

> Jinými slovy: k tomu, aby znemožnil práci s SHA-2, stačí jediný prvek celého řetězce, který SHA-2 nepodporuje.

Rozeberme si nyní podporu SHA-2 v produktech Microsoftu podle jednotlivých prvků celého řetězce.[15] Přitom budeme rozlišovat dva různé účely, protože jejich podpora se u konkrétních prvků může lišit:

- ověření certifikátu s SHA-2: toto je zapotřebí například v situaci, kdy se svým prohlížečem přistupujeme k nějakému serveru, který se nám prokazuje svým serverovým certifikátem – a ten byl vystaven s využitím SHA-2.
- ověření (vyhodnocení platnosti) nebo vytvoření elektronického podpisu na dokumentu či na e-mailové zprávě, na bázi SHA-2

7.5.1 Operační systém

Plnou podporu SHA-2, a to pro oba účely (ověření certifikátu, ověření a vytvoření podpisu), mají operační systémy MS Windows Vista a MS Windows7. Naopak operační systémy před MS Windows XP, tedy MS Windows 9x, MS Windows ME, MS Windows NT a MS Windows 2000 hašovací funkci SHA-2 nepodporují vůbec, a to ani pro jeden z obou výše uvedených účelů.

U samotného operačního systému MS Windows XP je třeba rozlišovat, o jakou verzi tzv. Service Packu (SP) je rozšířen. Pokud jde o SP1 nebo SP2, pak SHA-2 nepodporuje. Pokud jde o Windows XP, rozšířené o SP3, pak podporuje ověřování certifikátů na bázi SHA-2, ale nikoli již ověřování podpisů na dokumentech či zprávách na bázi SHA-2 či jejich vytváření.

---

[15] SHA-2 je ve skutečnosti celou rodinou hašovacích funkcí, které se liší velikostí otisku (hashe): 224, 256, 384 nebo 512 bitů. V produktech Microsoftu je implementována pouze trojice vyšších funkcí (SHA-256, SHA-384 a SHA-512). Funkce SHA-224, která ani není určena pro elektronický podpis, podporována není.

7.5.2 Aplikace

Podpora SHA-2 se poprvé objevuje v kancelářském balíku MS Office verze 2003 – ale jen u programu MS Outlook 2003 a jen pro ověřování podpisů s SHA-2 na přijatých zprávách. Nikoli ještě pro podepisování odesílaných zpráv.

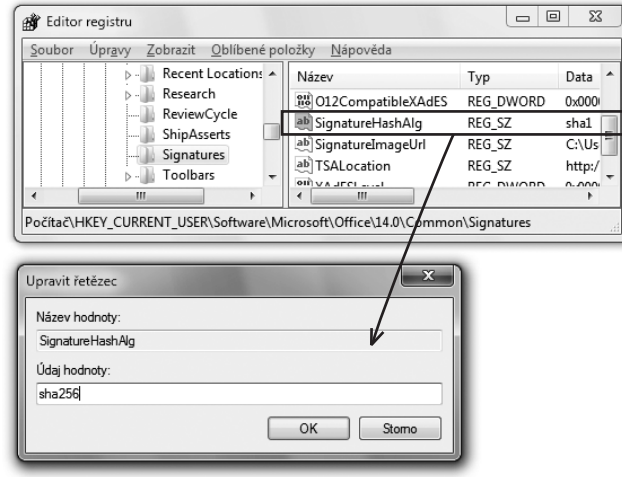
Plnou podporu SHA-2 mají až verze MS Office 2007 a 2010, a to jak pro podepisování dokumentů v programech MS Word, MS Excel a MS PowerPoint (a ve verzi 2010 i InfoPath), tak i pro podepisování e-mailových zpráv (MS Outlook).

O tom, zda při podepisování odesílaných zpráv (v MS Outlooku) bude použita ještě hašovací funkce SHA-1, nebo již novější SHA-2, rozhoduje nastavení v aktuálně používaném (výchozím) profilu, viz část 7.4.1.

Pro podepisování dokumentů (v programu MS Word a dalších) je standardně nastavena ještě původní hašovací funkce SHA-1. Mají-li nově vytvářené podpisy již používat SHA-2, je třeba tuto možnost nejprve explicitně zapnout (aktivovat). To lze udělat buďto vhodným nástrojem pro správu (je-li k dispozici), nebo nastavením položky SignatureHashAlg v registru, podle obrázku.

Přípustné hodnoty pro nastavení této položky jsou:

- sha1 (default)
- sha256
- sha384
- sha512



Obrázek 7-49
Změna obsahu registru tak, aby při podepisování dokumentů byla používána hašovací funkce SHA-2

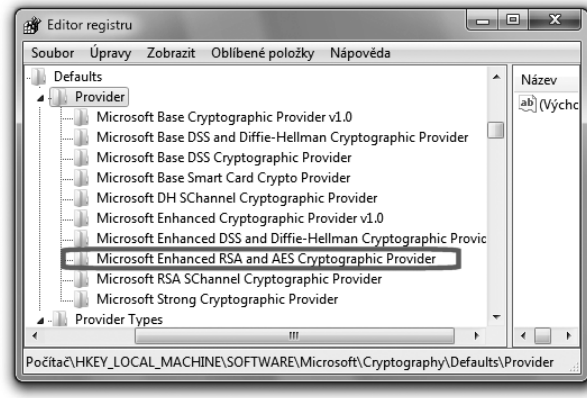
7.5.3 Moduly CSP

Připomeňme si, že moduly CSP (Cryptographic Service Provider) jsou prvky, které zprostředkovávají práci s certifikáty a klíči, a také různé kryptografické operace. Skrze ně jsou také „obsluhována“ jednotlivá úložiště důvěryhodných certifikátů. Lze si tedy představovat, že výběr úložiště souvisí s výběrem modulu CSP.

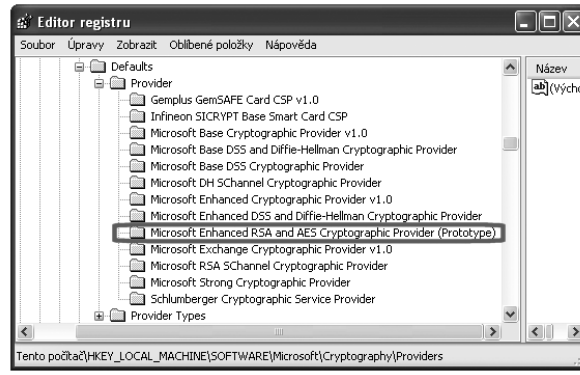
V operačním systému MS Windows je vždy obsažen určitý počet modulů CSP, které jsou „poskytnuty“ samotným operačním systémem. Vedle nich ale mohou být v systému další moduly CSP, poskytnuté třetími stranami a nainstalované při instalaci produktů těchto třetích stran (nejčastěji čipových karet či USB tokenů).

To, které moduly CSP jsou na konkrétním počítači právě dostupné, lze zjistit z tzv. registru. Příklad pro Windows XP s SP3 a pro Windows 7 ukazují obrázky.

Obrázek 7-50
Přehled modulů CSP, aktuálně dostupných na konkrétním počítači s MS Windows 7



Obrázek 7-51
Přehled modulů CSP, aktuálně dostupných na konkrétním počítači s MS Windows XP+SP3



Pro podporu SHA-2 za účelem ověřování a vytváření elektronických podpisů jsou důležité tzv. základní CSP moduly, které jsou používány pro podepisování.

Podporu pro SHA-2 však nabízí jen některé z nich. Konkrétně jde o modul **Microsoft Enhanced RSA and AES Cryptographic Provider**, který se ale vyskytuje jen u vyšších verzí operačního systému MS Windows, než jsou Windows XP+SP3.

V MS Windows XP s SP3 je místo tohoto CSP modulu jiný, který také podporuje SHA-2, a který se jmenuje téměř stejně – jen má na konci svého jména příponu (**Prototype**).

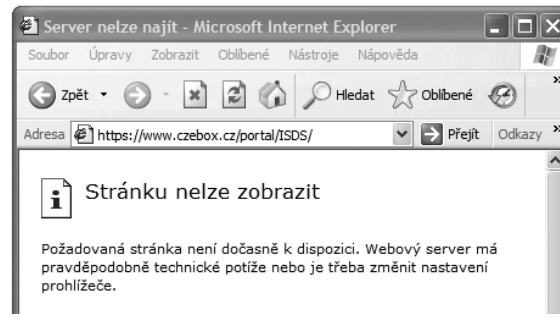
Toto může způsobovat problémy v situacích, kdy potřebujeme přenášet soukromé klíče a s nimi spojené certifikáty mezi různými verzemi operačních systémů.

S každým soukromým klíčem, instalovaným v úložišti, je totiž spojena informace o CSP modulu, který má být používán při použití tohoto klíče k podepisování.[16] Tato informace je k soukromému klíči logicky přidružena již v okamžiku generování žádosti o vystavení nového certifikátu – a pokud by stejný CSP modul nebyl k dispozici i na počítači, kam by soukromý klíč byl přenesen, resp. kde bude používán, musel by zde být použit jiný CSP modul (a to by mohlo být zdrojem problémů).

7.5.4 Příklady, kdy SHA-2 není podporována

Pro lepší docenění celé problematiky si nyní ukažme konkrétní příklady toho, kdy hašovací funkce SHA-2 není podporována.

Obrázek 7-52
Hlášení Internet Exploreru v situaci, kdy server používá serverový certifikát s SHA-2, ale klient SHA-2 nepodporuje



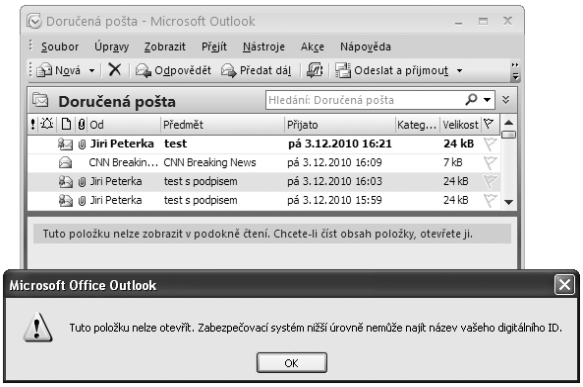
Například máme-li počítač se starším operačním systémem Windows než je XP, nebo právě XP s SP1 či SP2, nepodaří se nám dostat se na žádnou stránku takového serveru, který používá serverový certifikát s SHA-2. Důvodem je to, že tyto starší verze operačního systému nepodporují SHA-2 ani za účelem ověření certifikátu, a již z tohoto důvodu nedokáží navázat zabezpečenou komunikaci s takovýmto serverem.

16 Pro ověřování podpisu toto neplatí, zde se volba modulu CSP řídí jinými pravidly.

Jistým problémem je ale to, že uživatel se tento důvod nedozví. Třeba prohlížeč Internet Explorer v takovém případě nesprávně svádí chybu na server, místo toho aby ji viděl na své straně. Viz předchozí obrázek.

Dalším příkladem může být kombinace operačního systému MS Win-dows XP + SP3 a programu MS Outlook (lhostejno jaké verze). Tato verze operačního systému sice již SHA-2 z části podporuje, ale jen na úrovni ověření certifikátu. Nikoli již pro ověřování podpisů.

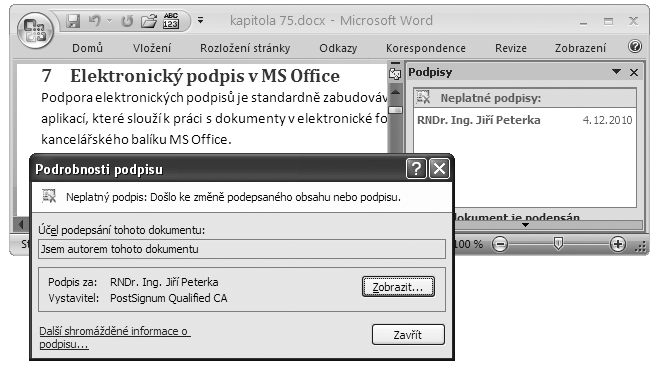
Obrázek 7-53
MS Outlook (nad Windows XP+SP3) nedokáže přečíst zprávu, podepsanou pomocí SHA-2



Příklad ukazuje předchozí obrázek, na kterém je MS Outlook 2007, běžící na počítači s MS Windows XP+SP3. Měl by zobrazit zprávu, opatřenou elektronickým podpisem na bázi SHA-2. Jelikož ale má „pod sebou“ takový operační systém, který SHA-2 nepodporuje, zprávu zobrazit nedokáže.

O něco lepší je situace s podpisem dokumentů: je-li nějaký dokument opatřen elektronickým podpisem s SHA-2, na počítači s operačním systémem MS Windows s SP3 nepůjde tento podpis ověřit (ani vytvořit). A to ani při použití programů (jako např. MS Word) verze 2007 či 2010, které podpisy s SHA-2 samy podporují.

Obrázek 7-54
Podpis s SHA-2 je na počítači s MS Windows XP+SP3 hodnocen jako neplatný



Příslušný podpis bude vyhodnocen jako neplatný z důvodu porušení integrity, viz předchozí obrázek. Na rozdíl od podepsané e-mailové zprávy ale je obsah takovéhoto dokumentu alespoň korektně zobrazen.

8. Šifrování, přihlašování a zabezpečená komunikace

Kapitola 8

8. Šifrování, přihlašování a zabezpečená komunikace

Metody, postupy a technologie, které jsme si v předchozích kapitolách popisovali v souvislosti s elektronickým podpisem, jsou poměrně univerzální a nachází čím dál tím větší uplatnění i jinde – v jiných oblastech a pro jiné účely, než je samotné podepisování, resp. vytváření a ověřování elektronických podpisů, elektronických značek a časových razítek.

A když už jsme se s těmito metodami, postupy a technologiemi seznámili, bylo by velkou škodou neříci si alespoň něco o možnostech jejich dalšího využití. Včetně konkrétních příkladů z každodenní praxe.

8.1 Šifrování

Jednou z možností, jak „jinak" využít metody a technologie z oblasti elektronického podpisu, je jakoby obrátit samotný postup podepisování – a tím dosáhnout efektu důvěrnosti pomocí šifrování.

Připomeňme si v této souvislosti, že **důvěrností** (anglicky **privacy**) rozumíme zajištění toho, aby naše data „zůstala důvěrná" a nemohl se s nimi seznámit nikdo, koho považujeme (v tomto ohledu) za nepovolaného.

Zajistit takovouto důvěrnost se v principu dá i omezením dostupnosti příslušných dat. Tedy tím, že svá data nepředáme (neumožníme získat, zkopírovat atd.) nikomu nepovolanému. To se ale v praxi těžko realizuje tam, kde svá data potřebujeme přenášet skrze takový přenosový kanál, u kterého nemáme záruku ohledně toho, kdo všechno se k přenášeným datům bude moci dostat. Třeba když je potřebujeme poslat běžnou elektronickou poštu, nebo předat mezi webovým serverem a jeho klientem skrze veřejný Internet.

V takovýchto případech nezbývá než řešit důvěrnost na jiném principu, konkrétně na bázi **šifrování** (anglicky: **encryption**). Tedy dopředu počítat s tím, že k našim datům se může dostat kdokoli – a zajistit, že se dostane jen k takové podobě, která mu stejně bude k ničemu. Tedy pouze k zašifrované podobě, kterou dokáže rozšifrovat (dešifrovat) jen oprávněná osoba, ale ta neoprávněná nikoli.[1]

8.1.1 Symetrické šifrování

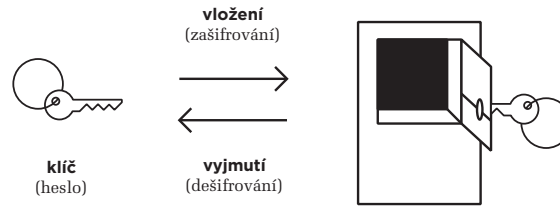
Podstatu šifrování si můžeme představit jako obdobu možnosti zamknout příslušná data do nějakého sejfu či trezoru – a klíč od něj dát jen tomu, kdo má být povolanou osobou.

V prvním přiblížení to může vypadat jako řešení důvěrnosti na principu omezené dostupnosti: možnost dostat se k datům dáme jen tomu, kdo bude mít klíč od trezoru. Jenže co když místo s daty budeme manipulovat přímo s celým trezorem? Tedy když budeme naše data potřebovat přenést přes nějaký (nezabezpečený) přenosový kanál, nebudeme je přenášet „tak jak jsou" (v „otevřené"

[1] Alternativou by mohlo být využití steganografie, při které jsou užitečná data „rozprostřena" tak, že je (bez dalšího) nelze rozpoznat a nelze ani detekovat, že nějaká data vůbec jsou přenášena.

podobě), ale budeme přenášet rovnou celý trezor. Pak nám může být celkem jedno, kdo všechno trezor po cestě zachytí (zkopíruje), když jej – bez klíče – nedokáže otevřít.

Obrázek 8-1
Představa symetrického šifrování



Tím jsme dosáhli efektu šifrování.

Právě naznačený postup přitom odpovídá takovému šifrování, které je označováno jako **symetrické**. Neboli takové, které se opírá o **symetrickou kryptografii**. Důležité je, že „symetričnost" je zde dána tím, že od trezoru s daty existuje jen jeden klíč, který používá jak odesilatel (přesněji: ten, kdo šifruje), tak i příjemce (přesněji: ten kdo dešifruje). Proto symetrie a symetrické šifrování, resp. symetrická kryptografie.

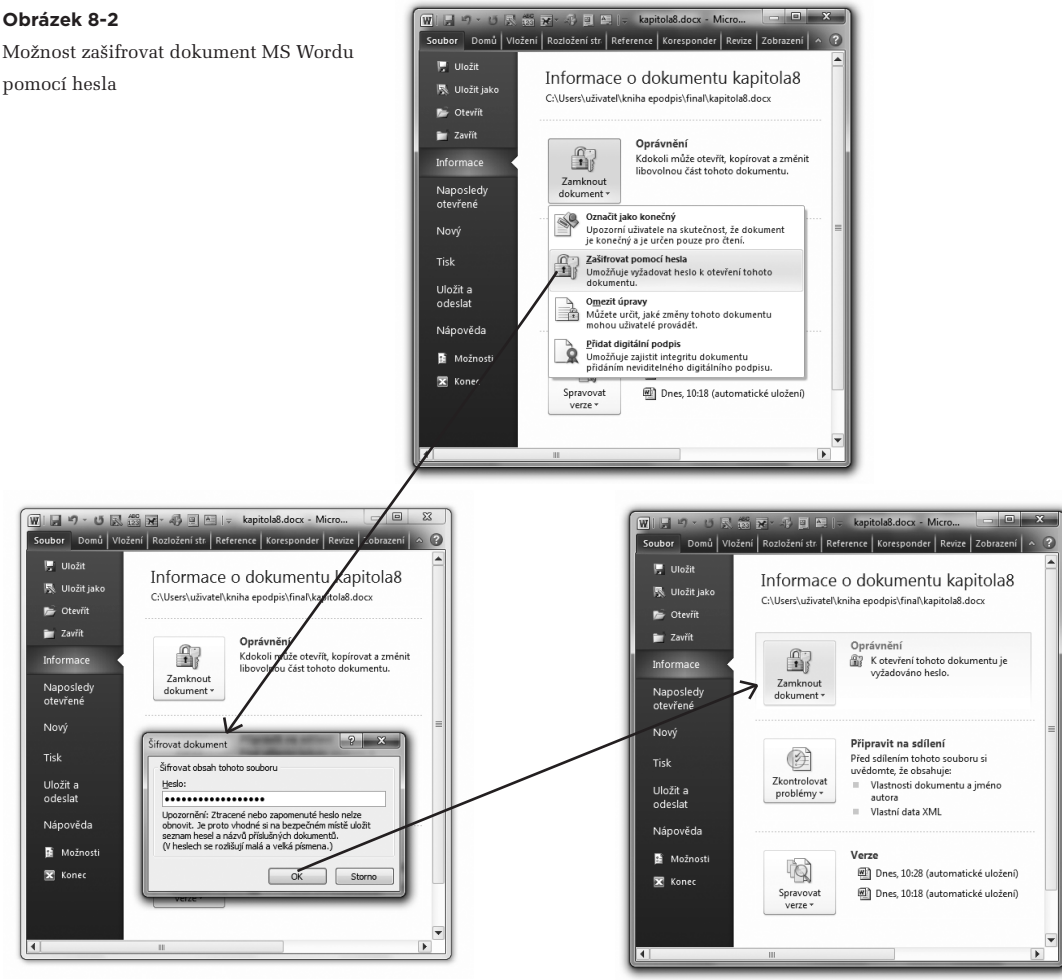
V praxi se symetrické šifrování skutečně používá. Má navíc i jednu významnou výhodu (oproti asymetrickému šifrování, se kterým se seznámíme záhy): je výpočetně mnohem méně náročné. Symetrické šifrování a dešifrování je tedy relativně nenáročné na kapacitu a zdroje našich počítačů.

Praktický příklad si můžeme ukázat na možnosti zašifrovat dokument v rámci kancelářského balíku MS Office: přes příslušné ikonky v menu se dostanete k nabídce, umožňující zašifrovat aktuální dokument.

Program z MS Office po vás ale nebude chtít klíč (požadovaného formátu a velikosti), nýbrž jen heslo, ze kterého si klíč sám vyrobí. Efekt ale bude stejný, jako kdyby (symetricky) šifroval rovnou heslem: přístup k dokumentu bude mít jen ten, kdo bude znát (držet, vlastnit) příslušné heslo. Jinak se k obsahu dokumentu nedostane – i když s dokumentem jako takovým bude moci manipulovat jako s celkem (tedy třeba jej kopírovat z místa na místo, odesílat elektronickou poštou apod.).

Na druhou stranu má symetrické šifrování jednu zásadní nevýhodu: jelikož od (pomyslného) trezoru existuje jen jeden (symetrický) klíč, je nutné zajistit jeho bezpečnou **distribuci** – tak, aby se dostal právě a pouze do povolaných rukou. Což nemusí být vůbec jednoduché. A když už bude klíč v povolaných rukou, je nutné pohlídat i to, aby v nich zůstal a nedostal se do nepovolaných rukou. Tedy pečlivě jej chránit a udržovat v tajnosti. Proto se o tomto klíči hovoří také jako o **tajném klíči.**

Obrázek 8-2
Možnost zašifrovat dokument MS Wordu pomocí hesla



8.1.2 Asymetrické šifrování

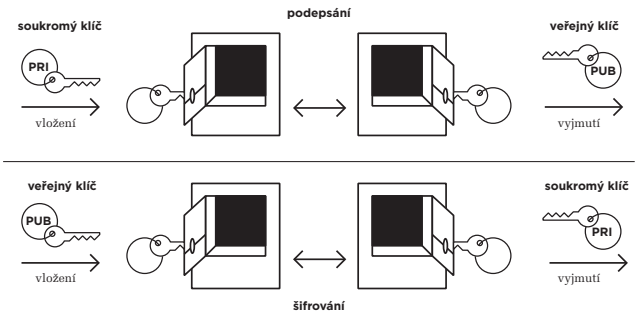
Pro bezpečnou distribuci tajných klíčů samozřejmě existuje více možností. Například když někoho známe osobně a nacházíme se v jeho přímé blízkosti, můžeme mu tajný klíč předat „z ruky do ruky“ a tím vše snadno vyřídit.

Pokud ale nejsme v jeho blízkosti, budeme potřebovat nějaký spolehlivý přenosový kanál tak, aby při přenosu nedošlo ke kompromitaci tajného klíče (aby se nedostal do nepovolaných rukou). Takový kanál by měl přenášená data šifrovat – ale tím se dostáváme do nepříjemného kruhu (kdy k zajištění šifrování potřebujeme již fungující šifrování).

Ještě nepříjemnějším problémem ale může být to, když dotyčného či dotyčnou vůbec neznáme. Jak se potom vyvarovat nebezpečí, že bychom tajný klíč předali někomu jinému, kdo se za zamýšleného a správného příjemce jen vydává? Zde bychom potřebovali někoho třetího, komu dostatečně důvěřujeme, a kdo by nám určitým způsobem zprostředkoval předání – buďto samotných dat, nebo alespoň (symetrického) klíče – do rukou té správné osoby, za jejíž identitu bude ručit.

Svým způsobem je to velmi podobné tomu, co jsme potřebovali u elektronického podpisu: tam jsme při ověřování podpisu použili veřejný klíč a od certifikační autority jsme chtěli, aby nám (skrze vydaný certifikát) ručila za identitu toho, komu veřejný klíč patří. Nyní ale vše jakoby obrátíme: veřejný klíč nepoužijeme k ověření podpisu ale k zašifrování toho, co potřebujeme zašifrovat. A díky podstatě asymetrické kryptografie, konkrétně díky vazbě mezi soukromým a veřejným klíčem, budeme mít zajištěno, že takto zašifrovaná data bude moci dešifrovat pouze ten, kdo vládne odpovídajícím soukromým klíčem. Tedy ten, komu byl certifikát vystaven.

Připomeňme si to na následujícím obrázku, který jsme si ukazovali již v části 3.2. Je na něm představa využití asymetrické kryptografie pro podepisování a pro šifrování:



Obrázek 8-3
Představa využití asymetrické kryptografie pro podepisování a pro šifrování

Oba úkony si podle tohoto obrázku lze představit jako vkládání (dokumentu, dat) do obdobného trezoru, sejfu či bezpečnostní schránky jako u symetrického šifrování – ale s tím podstatným rozdílem, že nyní má tento trezor dvě jednosměrná dvířka: jedněmi lze pouze vkládat, zatímco druhými lze pouze vybírat (vyjímat). A každá dvířka se otevírají jiným klíčem: buďto soukromým klíčem, nebo veřejným klíčem.

Úkonu podepisování pak odpovídá vložení těmi dvířky, které se odemykají soukromým klíčem. Díky tomu je zajištěno, že vyjmutí ze schránky (které odpovídá ověření podpisu) lze provést jen skrze druhá dvířka, která se otevírají veřejným klíčem. Podrobněji viz kapitola 3.

Nás zde ale zajímá „obrácený“ postup, který naznačuje spodní část předchozího obrázku: do trezoru se dokument či jakákoli jiná data vloží těmi dvířky, které otevírá veřejný klíč. Přesněji veřejný klíč té osoby, „pro kterou“ šifrujeme a která je zamýšleným příjemcem dokumentu či dat – protože pouze tato osoba bude schopna vyjmout dokument či data z trezoru druhými dvířky, které si odemkne pomocí svého soukromého klíče. A díky unikátní vazbě mezi soukromým a veřejným klíčem můžeme mít jistotu, že nikdo jiný (bez odpovídajícího soukromého klíče) to nebude moci udělat.

Povšimněme si zde zajímavého a důležitého rozdílu: zatímco u symetrického šifrování se může šifrovat jakoby „obecně“ – pro kohokoli, kdo bude znát heslo (resp. tajný klíč), u asymetrického šifrování se šifruje „cíleně“ – pro konkrétního příjemce.[2]

Dalším důsledkem může být to, že je-li stejný dokument určen pro více různých osob (příjemců), v případě asymetrického šifrování je šifrován individuálně pro každého jednotlivého příjemce, pomocí jeho veřejného klíče. V případě symetrického šifrování stačí dokument zašifrovat jen jednou a příslušný klíč doručit všem příjemcům.[3]

Zdůrazněme si také další přednost, se kterou jsme vlastně začínali popis asymetrického šifrování: že u něj odpadá problém s distribucí tajných klíčů. Díky principům PKI (infrastruktury veřejných klíčů) a důvěryhodným certifikačním autoritám je distribuce veřejných klíčů bezproblémová, zatímco soukromé klíče se nedistribuují vůbec.

Stejně tak si připomeňme, že pro šifrování musíme používat komerční certifikáty, a nikoli certifikáty kvalifikované.

Důvody toho, proč k šifrování nesmíme používat kvalifikované certifikáty, vychází přímo ze zákona (č. 227/2000 Sb., o elektronickém podpisu) a jsou explicitně formulovány i v certifikačních politikách a obchodních podmínkách certifikačních autorit, které vystavují kvalifikované certifikáty. Podrobněji viz část 4.3.6.

> Příkladem mohou být odlišné podmínky nakládání se soukromým klíčem, který se váže buďto ke komerčnímu, nebo ke kvalifikovanému certifikátu. V prvním případě jej můžeme bez větších problémů zálohovat, a měli bychom tak činit (abychom se vůbec ještě dostali k tomu, co jsme si zašifrovali sami, nebo co zašifroval někdo pro nás). Dokonce jej můžeme svěřit do úschovy někomu jinému (třeba i zaměstnavateli), aby se v případě potřeby (nemoci, úmrtí apod.) k zašifrovaným datům mohl také dostat. Ve druhém případě je zálohování soukromého klíče mnohem problematičtější a soukromý klíč vůbec nesmíme předávat někomu jinému.

8.1.3 Šifrování v programu MS Outlook

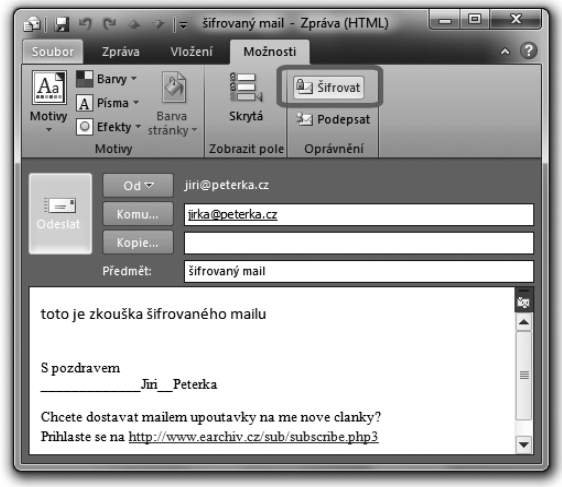
Konkrétní využití asymetrického šifrování si můžeme ukázat na příkladu poštovního klienta Outlook z kancelářského balíku MS Office verze 2010. Pokud je vše řádně připraveno, je samotné zašifrování nově odesílané zprávy triviální: stačí stisknout tlačítko „Šifrovat“, které je standardně umístěno na kartě „Možnosti“, viz obrázek.

---

[2] I když toto může ve skutečnosti znamenat, že (z důvodu efektivnosti) je samotný obsah zašifrován „symetricky“, pomocí tajného klíče, a teprve tento tajný klíč je zašifrován „asymetricky“ a individuálně pro příslušného příjemce.

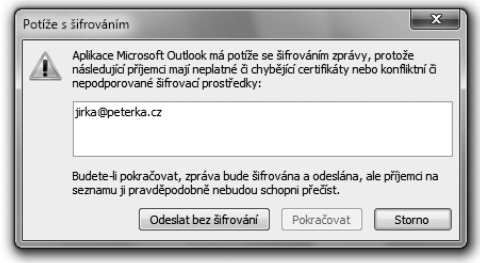
[3] Toto je jednodušší, ale méně bezpečná varianta: s větším počtem příjemcům tajného klíče roste nebezpečí jeho prozrazení. Větší bezpečnost skýtá varianta, kdy je použito více tajných klíčů (na každého příjemce jeden). Pak ale musí být stejný dokument zašifrován také tolikrát, kolik je příjemců.

Obrázek 8-4
Požadavek na šifrování nové zprávy v MS Outlook



Jenže aby Outlook mohl tomuto požadavku vyhovět, musí mít k dispozici certifikát s veřejným klíčem příjemce, resp. všech příjemců (neboť pro každého vypravuje samostatný a individualizovaný exemplář zprávy). Pokud žádný takový certifikát nenajde, nebo s ním má nějaký problém, ohlásí to uživateli a dá mu na výběr, zda chce zprávu odeslat nezašifrovanou, nebo ji neodesílat vůbec.

Obrázek 8-5
Hlášení MS Outlooku, že k uvedené e-mailové adrese nenalezl certifikát s veřejným klíčem

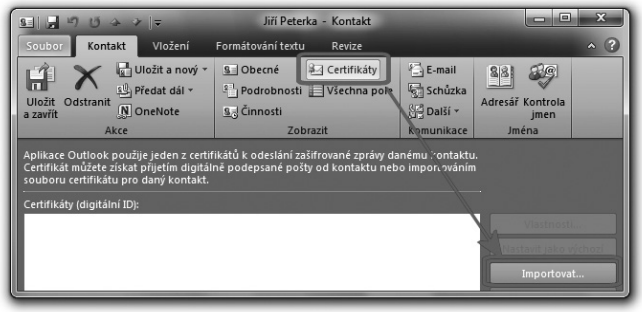


Kde ale Outlook hledá certifikáty, které potřebuje k šifrování?

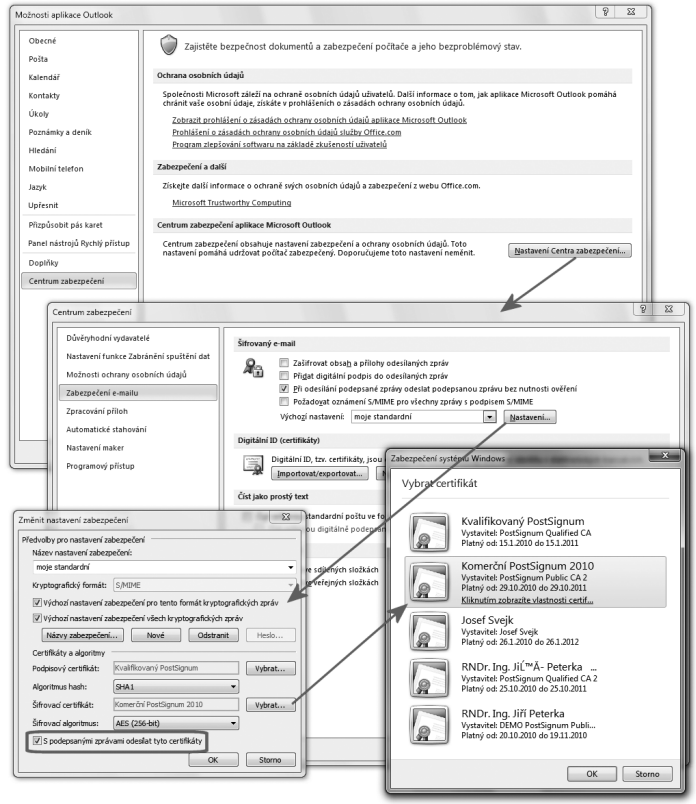
Kupodivu nikoli v systémovém úložišti MS Windows, které dokonce má složku pro certifikáty jiných uživatelů (s názvem „Ostatní uživatelé“). Místo toho Outlook hledá certifikáty pro šifrování e-mailů na dvou místech:

- v aktuálně používaném adresáři kontaktů, nebo
- přímo ve zprávě, na kterou odpovídá (pokud jde o odpověď)

První možnost je vhodná pro případ, kdy něčí certifikát získáte přímo. Například když vám jej někdo předá „z ruky do ruky“. Pak si jej můžete sami připojit k příslušnému kontaktu v aktuálně používaném adresáři.



Obrázek 8-6
Přidání certifikátu ke kontaktu v adresáři

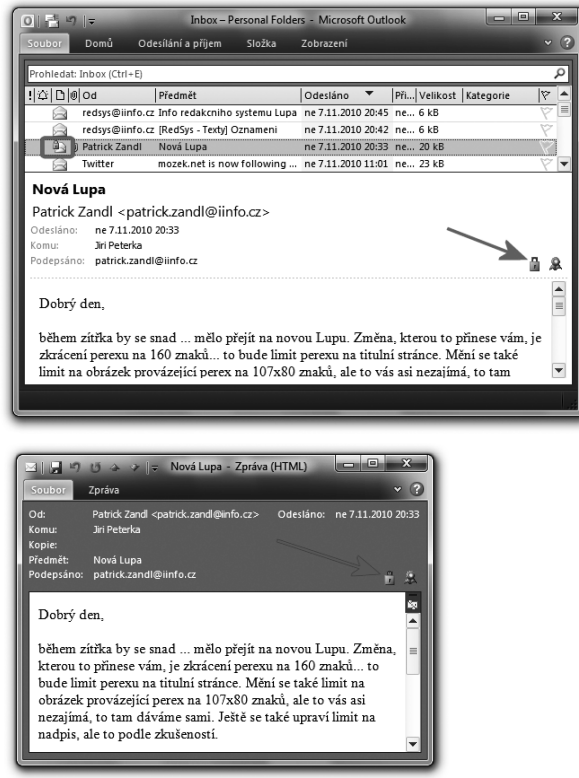


Obrázek 8-7
Nastavení zabezpečení – s volbou certifikátu, který bude automaticky vkládán do podepsané zprávy

Druhá možnost bude asi v praxi mnohem častější. Počítá s tím, že protistraně sami a „dopředu“ pošlete svůj šifrovací certifikát, aby jej měla k dispozici pro případ, že bude chtít zašifrovat svou odpověď.

Konkrétně že svůj šifrovací certifikát necháte automaticky vložit přímo do odesílané zprávy (pokud bude současně elektronicky podepisována). Klientský poštovní program protistrany jej zde najde a bude jej tak mít ihned k dispozici pro případ, že dostane za úkol zašifrovat odpověď, která se bude vracet k vám. Příklad nastavení MS Outlooku pro tuto volbu ukazuje předchozí obrázek.

Pokud naopak sami dostanete nějakou zašifrovanou zprávu, poznáte to snadno podle charakteristické modré ikonky ve tvaru visacího zámku, kterou MS Outlook signalizuje šifrovanou zprávu.



Obrázek 8-8
Zobrazení šifrované zprávy ve výpisu zpráv v MS Outlook

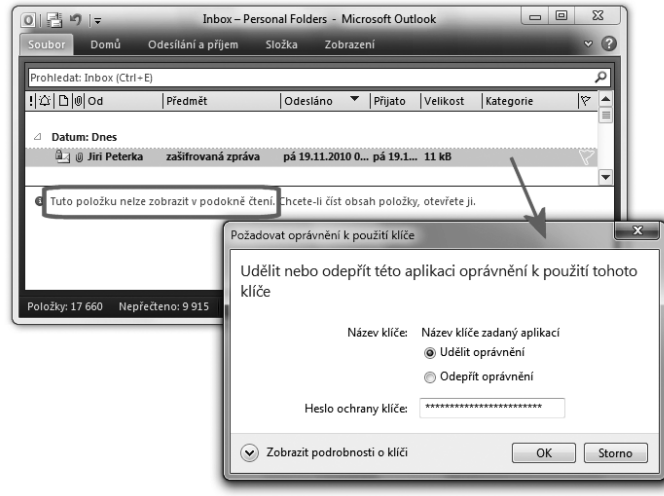
Kliknutím na modrou ikonku, indikující šifrovanou zprávu, lze vyvolat zobrazení detailů o podpisu i šifrování e-mailové zprávy.

Odsud je pak možné zjistit, se kterým certifikátem je šifrování spojeno. Přesněji který certifikát (a v něm obsažený veřejný klíč) byl pro šifrování použit. Podle toho pak i Outlook sám vybírá soukromý klíč, který potřebuje pro dešifrování obsahu zprávy.

Důležité přitom je, aby Outlook příslušný soukromý klíč našel, a také aby k němu získal přístup (což může vyžadovat zadání správného hesla uživatelem, pokud je jím soukromý klíč chráněn). Pokud se to Outlooku nepodaří, není schopen zašifrovanou zprávu dešifrovat – a její obsah tudíž nedokáže svému uživateli zobrazit.

Na tuto skutečnost je třeba pamatovat při hospodaření s certifikáty. Pokud si třeba nenávratně smažete ten certifikát, kterým jsou zašifrovány přijaté e-mailové zprávy, již se k jejich obsahu nedostanete.

Na druhou stranu, pokud Outlook má potřebný certifikát k dispozici, použije jej a ukáže vám obsah zprávy i v případě, kdy platnost tohoto certifikátu již skončila.



Obrázek 8-9
Pro zobrazení zašifrované zprávy je třeba přístup k soukromému klíči

8.2 Přihlašování

Dalším účelem, ke kterému se technologie elektronického podpisu používají, a to čím dál tím častěji, je potřeba identifikace a autentizace. Například při přihlašování uživatele k nějaké on-line službě, ale obecně všude tam, kde se jedna strana potřebuje představit druhé straně (říci kým je, neboli: identifikovat se) a současně prokázat, že je skutečně tím, za koho se vydává (autentizovat se, provést autentizaci).

Pro identifikaci a autentizaci samozřejmě existuje řada různých metod a technik, které jsou „různě silné“, ve smyslu své spolehlivosti a možnosti nějakého podvržení či podvodu. Historicky nejstarší, ale přesto stále používaná, je identifikace pomocí uživatelského jména a autentizace pomocí hesla. Ale snad netřeba podrobněji rozvádět, jak málo je tato varianta bezpečná. Jak snadné je někde odposlechnout či jen „odkouknout“ něčí jméno a heslo, a pak jej zneužít.

Proto se stále častěji přechází na sofistikovanější metody autentizace (prokázání vlastní identity), které skýtají podstatně vyšší míru bezpečnosti a ochrany proti zneužití a podvodům. Tyto metody se obecně snaží „zapojit do hry“ co možná nejvíce dalších faktorů, které se pak spolupodílejí na autentizaci. Proto se v této souvislosti hovoří o **vícefaktorové autentizaci**.

Takovým dalším faktorem může být „něco, co uživatel právě drží“, resp. má ve své moci a může s tím nakládat. Což může být například soukromý klíč, kterým disponuje právě (a pouze) uživatel.[4] Proč jej tedy nevyužít ke zvýšení spolehlivosti a bezpečnosti autentizace? A s ním i certifikáty, které jsou se soukromým klíčem spojeny?

Způsob, jakým soukromý klíč „zapojit do hry“ i pro potřeby autentizace, je principiálně velmi jednoduchý a vychází ze základního principu asymetrické kryptografie, který jsme si již vícekrát popisovali: že soukromý klíč a veřejný klíč (obsažený v certifikátu) jsou „do páru“ a co lze „zamknout“ jedním z nich, lze „odemknout“ právě a pouze tím druhým. Navíc s vědomím toho, že soukromý klíč uživatel nesmí „dát z ruky“, a tak s ním může cokoli „uzamykat“ či naopak „odemykat“ jen u sebe. Naproti tomu svůj veřejný klíč (jako součást svého certifikátu) může předat protistraně, aby s ním mohla „odemykat“ či „zamykat“ ona.

Pak již zbývá jen vybrat si, který z klíčů bude použit dříve. V úvahu tedy připadají dva možné scénáře, ve kterýchpro jednoduchost nazývejme přihlašujícího se uživatele klientem, a protistranu serverem:

- server pošle klientovi „něco“, co klient „uzamkne“ svým soukromým klíčem a vrátí serveru, spolu se svým certifikátem. Server využije veřejný klíč z certifikátu, a s ním „odemkne“ to, co mu klient vrátil.
- klient nejprve pošle serveru svůj certifikát. Server využije veřejný klíč, který je v certifikátu obsažen, a s ním „uzamkne“ obdobné „něco“, co následně pošle klientovi. Ten toto „něco“ zase „odemkne“ pomocí svého soukromého klíče a odemčené vrátí zpět serveru.

Oba tyto scénáře implementují metodu, označovanou jako **metoda výzvy a odpovědi** (anglicky: **challenge-response**): jedna strana pošle druhé „výzvu“, a ta na ni zareaguje svou „odpovědí“.

V případě prvního scénáře je touto výzvou nějaký (obvykle náhodný) „kus dat“, který server zašle klientovi. Klient jej podepíše, neboli opatří svým elektronickým podpisem (k čemuž potřebuje svůj soukromý klíč) a přidá ještě svůj certifikát. Tím vzniká odpověď, která se vrací serveru – a ten si ověří podpis pomocí veřejného klíče z certifikátu.

V případě druhého scénáře pak nejde o podepisování, ale o šifrování: server nejprve zašifruje svůj „kus dat“, a teprve tím vzniká výzva, kterou zašle klientovi. Ten ji musí správně dešifrovat (pomocí

[4] Další možností je využít „něco, co uživatel zná“ (například nějaké heslo, jednorázový kód apod.) či „něco, čím uživatel je“, jako například otisk jeho prstu, vzorek sítnice apod.

svého soukromého klíče), a pak vrátit serveru jako svou odpověď. Server si pak zkontroluje, zda se shoduje s původním „kusem dat“.

V praxi se dnes používá téměř výlučně první ze zde uváděných scénářů, jelikož má oproti tomu druhému některé významné přednosti. Například tu, že certifikát klienta (přihlašujícího se uživatele) není třeba posílat nějak „dopředu“ (aby mohl být využit při šifrování v rámci druhého scénáře), ale stačí jej poslat až spolu s odpovědí.

Samotnou výzvou (resp. „kusem dat“), která se posílá v rámci prvního scénáře, bývá v praxi nějaká náhodně generovaná hodnota, resp. řetězec bitů, doplněná o časový údaj (resp. časové razítko). To proto, aby se ještě více znesnadnilo případné zneužití a podvody.

8.2.1 Registrace uživatelského certifikátu

Z čistě uživatelského pohledu ale není konkrétní dialog mezi serverem a klientem (včetně charakteru výzvy a odpovědi) obvykle patrný. Místo toho se od uživatele obvykle očekává něco jiného: že si u protistrany (u serveru) nejprve tzv. zaregistruje svůj osobní (neboli uživatelský) certifikát.

Důvod je ryze praktický: protistrana (server) nemusí být schopna jej identifikovat pouze na základě obsahu jeho certifikátu. Třeba proto, že v certifikátu je uvedeno (občanské) jméno a příjmení, zatímco server „zná“ uživatele pod nějakým (třeba úplně jiným) uživatelským jménem. Kvůli tomu musí být nejprve vytvořena vazba mezi uživatelským účtem na příslušném serveru a certifikátem, prostřednictvím kterého se uživatel bude přihlašovat.

Potřebné zaregistrování uživatelského certifikátu se proto provádí v době, kdy uživatel již je přihlášen ke svému účtu (takovým způsobem, jaký je pro něj momentálně dostupný, třeba jen pomocí jména a hesla). Celý úkon je přitom principiálně velmi jednoduchý: uživatel jen serveru „ukáže“ (předloží) ten certifikát, prostřednictvím kterého se chce nově přihlašovat. Jakoby tedy říkal: „*jsem to já, jen když se prokážu tímto certifikátem.*“

Připomeňme si, že ani pro potřeby přihlašování (resp. identifikace a autentizace uživatele vůči serveru či službě) nesmíme používat kvalifikované certifikáty. Zbývají tedy certifikáty komerční, jak obecně označujeme ty certifikáty, které nejsou kvalifikované.

Tentokráte je proti použití kvalifikovaných certifikátů i jednoduchý a pádný argument: při autentizaci podepisuje uživatel (v roli klienta) výzvu protistrany (serveru). Obsah této výzvy ale nevidí, a tak vlastně neví, co podepisuje.[5] Proto by nemělo jít o skutečný (ve smyslu: právně závazný) podpis, založený na kvalifikovaném certifikátu.

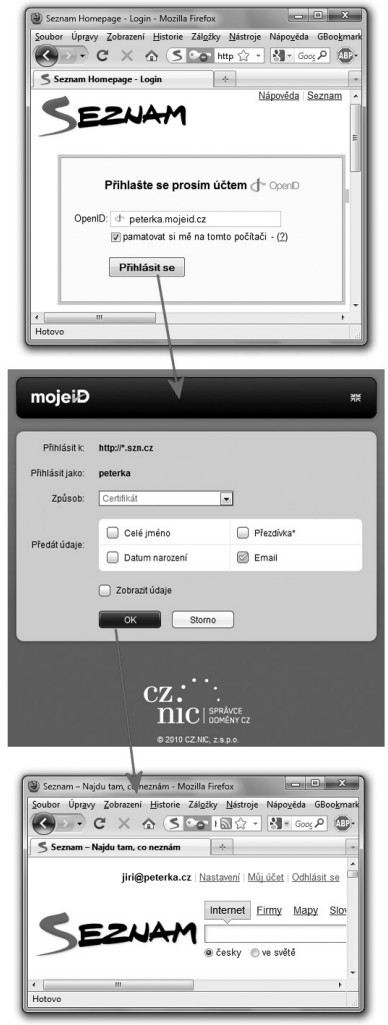
---

[5] Server může přihlašujícímu se uživateli „podstrčit“ otisk prakticky libovolného dokumentu. Pokud by přihlašující se uživatel používal kvalifikovaný certifikát, vlastně by tak příslušný dokument platně podepisoval.

8.2.2 Přihlašování ke službě MojeID prostřednictvím certifikátu

Prvním konkrétním příkladem, který si můžeme ukázat, je přihlašování pomocí certifikátu ke službě **MojeID**, provozované na adrese *http://mojeid.cz*.

Jde o službu pro jednotné přihlašování, založenou na technologii OpenID. Její podstatu si můžeme velmi stručně přiblížit tak, že umožňuje nahradit specifické přihlašování (k různým uživatelským účtům na různých serverech, pomocí různých uživatelských jmen a hesel) jednotným přihlášením pomocí jednoho jména a hesla. Nebo, což nás právě zde zajímá, pomocí jednoho uživatelského certifikátu.



Obrázek 8-10
Představa fungování služby MojeID

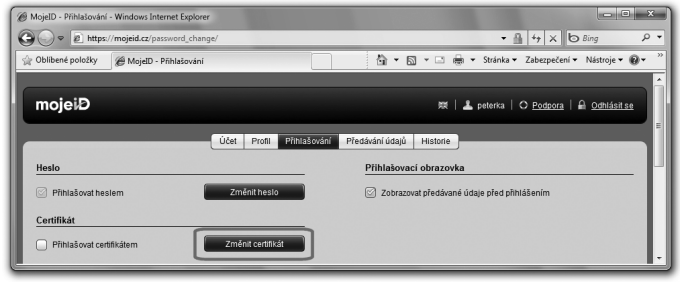
Princip, na kterém služba MojeID funguje, není nepodobný tomu, jak na Internetu funguje (zabezpečené) placení pomocí platebních karet: číslo své karty a další údaje nezadáváte přímo obchodníkovi, ale až zabezpečené platební bráně, na kterou jste od obchodníka přesměrováni. Teprve zde zadáte vše potřebné (a to jednotným způsobem, bez ohledu na to, komu vlastně platíte), načež jste zase přesměrováni zpět k původnímu obchodníkovi. Ten se vlastně ani nedozví, jakou platební kartou jste platili – ale dozví se to, zda od vás dostane požadovanou platbu.

V případě služby MojeID to funguje obdobně, jen místo plateb a peněz jde o přihlašování a vaše údaje: obdobou platební brány je přihlašovací stránka služby MojeID, na kterou jste přesměrováni a ke které se teprve přihlašujete. No a ona vás pak sama přihlásí k tomu serveru resp. službě, ze které jste původně přišli. Přitom jí předá takové údaje o vaší identitě, jaké služba požaduje a jaké vy jako uživatel odsouhlasíte. Představu s přihlašováním k serveru Seznam ukazuje předchozí obrázek.

K samotné službě MojeID se přitom lze přihlašovat jak jménem a heslem, tak i prostřednictvím certifikátu. V tomto druhém případě samozřejmě musíte nejprve zaregistrovat u služby MojeID svůj uživatelský certifikát tak, aby si jej služba dokázala „spojit“ s vaší identitou.

Možnost nově si zaregistrovat uživatelský certifikát (nebo změnit již zaregistrovaný) je u služby MojeID dostupná v rámci profilu uživatele, viz následující obrázek.

Obrázek 8-11
Možnost registrace uživatelského certifikátu u služby MojeID

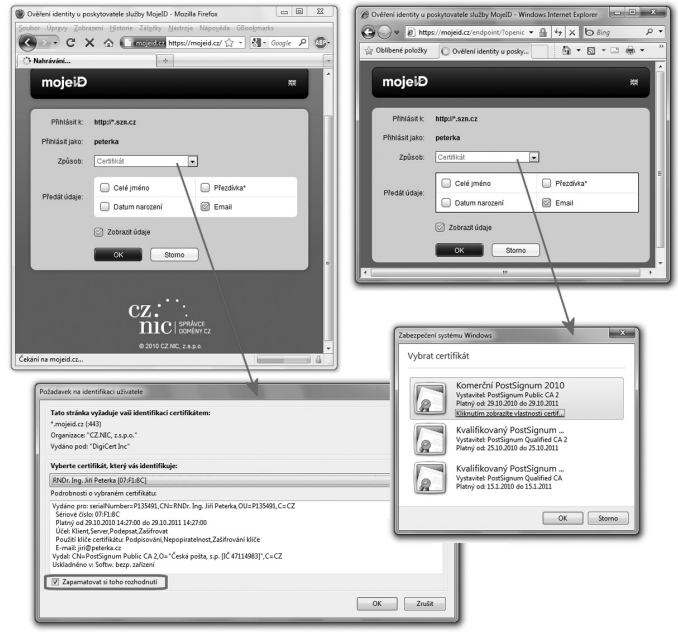


Samotná registrace certifikátu je pak relativně přímočará a jednoduchá. Náročnější ale může být požadavek na to, aby certifikát byl ve formátu PEM (Privacy Enhanced Mail).

Tento formát jsme si popisovali v části 5.3.1.2, proto jen stručné připomenutí, že jde o tvar dle standardu X.509 v kódování Base-64, nejčastěji ukládaný do souborů s příponou .cer. Export certifikátu ze systémového úložiště MS Windows do tohoto formátu naznačuje následující obrázek (vlevo).

Jakmile je uživatelský certifikát zaregistrován, může jej uživatel použít pro své přihlašování, ať již k samotné službě MojeID (například pro editaci svého profilu) či jejím prostřednictvím k jiným službám. Vždy přitom má na výběr, zda využije přihlášení prostřednictvím jména a hesla, nebo prostřednictvím certifikátu.

Obrázek 8-12
Export uživatelského certifikátu do formátu PEM a jeho registrace u služby MojeID



Obrázek 8-13
Přihlášení ke službě MojeID prostřednictvím certifikátu (z prohlížečů Firefox a Internet Explorer)

Pokud se uživatel přihlašuje pomocí certifikátu, jeho prohlížeč mu nabídne výčet těch, které jsou pro něj v danou chvíli dostupné a které považuje za použitelné pro účel přihlášení. Stále je ale na uživateli, aby vybral ten správný certifikát (který dříve zaregistroval jako svůj uživatelský u služby MojeID). Některé prohlížeče (na obrázku tuto možnost nabízí Firefox) si jeho volbu mohou pamatovat, příště ji prostě použít a nepožadovat novou volbu certifikátu.

8.2.3 Přihlašování k datovým schránkám pomocí certifikátu

Druhým příkladem, který si můžeme ukázat, je přihlašování k webovému rozhraní (portálu) datových schránek prostřednictvím certifikátu.

Nejprve si ale zdůrazněme, že datové schránky a jejich informační systém[6] byly spuštěny s tím, že základní způsob přihlašování k nim je pouze prostřednictvím jména a hesla.[7] A to i přesto, že právní úkony (podání), činěné prostřednictvím datových schránek, mají stejnou právní závaznost jako úkony podepsané, neboli opatřené platným (elektronickým) podpisem.[8]

Možnost přihlašovat se k datovým schránkám prostřednictvím certifikátu je tudíž pro běžné koncové uživatele pouze volitelnou možností, nikoli povinností. Dostupné statistiky přitom naznačují, že tato možnost je v praxi využívána jen zcela minimálně.

Způsob, jakým informační systém datových schránek pojímá přihlašování prostřednictvím datových schránek, odpovídá vícefaktorové autentizaci. V tom smyslu, že povinnost používat jméno a heslo nadále zůstává, a certifikát slouží (vedle jména a hesla) jako další prvek autentizace. Není to tedy tak, že by použití certifikátu nahrazovalo použití hesla.[9]

Nejméně poprvé se ale každý uživatel musí přihlásit ke své datové schránce jen pomocí jména a hesla. To proto, aby si mohl zaregistrovat svůj uživatelský certifikát, a pak se přihlašovat s jeho pomocí.

Jakmile si ale uživatel jednou zaregistruje svůj certifikát, již se dále nemůže přihlašovat jen pomocí jména a hesla, jako původně (ale jen s pomocí certifikátu). Proto existuje i možnost zrušit registraci uživatelského certifikátu, tak aby se uživatel opět mohl přihlašovat jen prostřednictvím jména a hesla. Obě možnosti je třeba hledat v části pro nastavení datové schránky, a zde pak v části věnované správě certifikátů – kterou ukazuje následující obrázek.

---

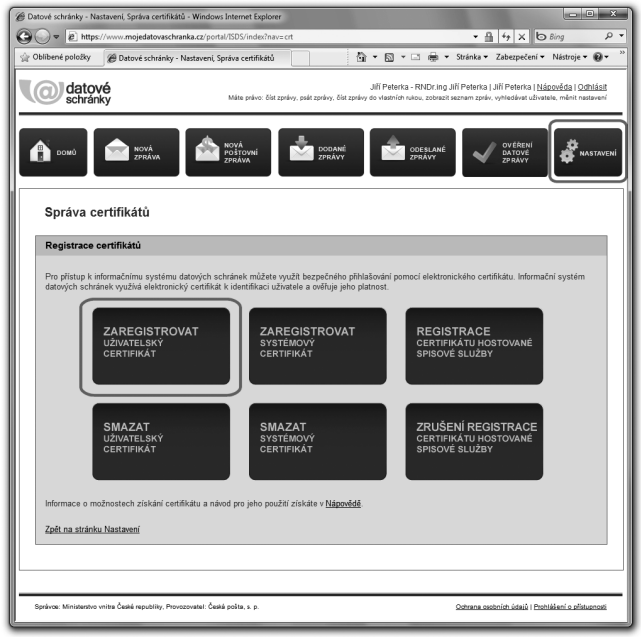
6 Informační systém datových schránek, zkratkou ISDS.

7 Toto heslo musí uživatel každých 90 dnů měnit. Nově ale má možnost tuto povinnosti vypnout, a heslo pak měnit nemusí.

8 Díky tzv. fikci elektronického podpisu, neboli ustanovení §18/2 zákona č. 300/2008 Sb., který říká, že úkon učiněný prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný.

9 Použití certifikátu nahrazuje pouze systém captcha, používaný při přihlašování (pouze) jménem a heslem.

Obrázek 8-14
Nabídka registrace certifikátů v nastavení datové schránky



Možnost zrušení registrace je sice prezentována jako smazání certifikátu, ale to se skutečně týká jen registrace u samotné datové schránky (a uživatel o certifikát ve svém úložišti samozřejmě nepřijde).

Samotné zaregistrování uživatelského certifikátu je pak ještě jednodušší než u předchozího příkladu se službou MojeID: uživatel zde nemusí sám vyhledávat svůj certifikát v požadovaném formátu, ale je mu rovnou nabídnut výčet těch, které jsou pro právě používaný prohlížeč dostupné (v jím používaném úložišti). Příklad ukazuje obrázek 8-15 na další stránce.

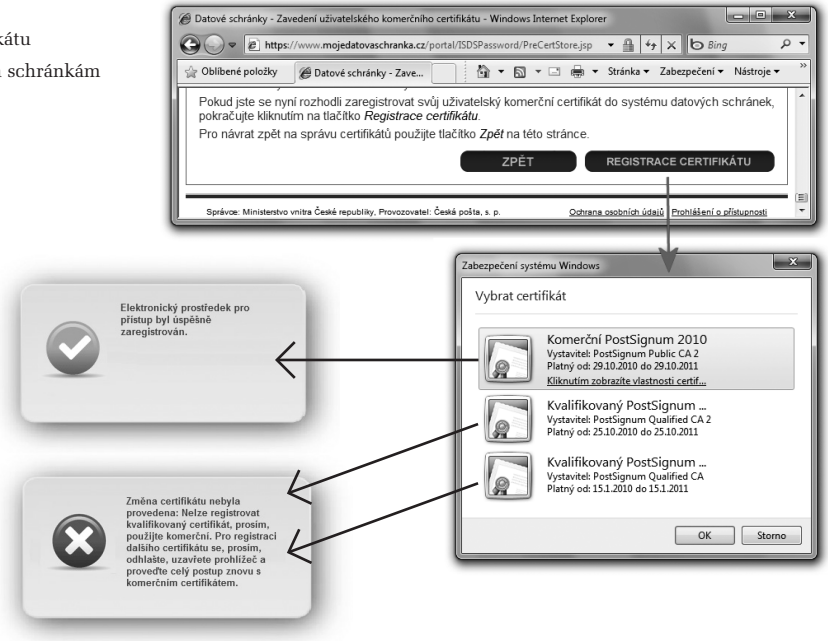
Připomeňme si znovu, že k přihlašování je (obecně) třeba využívat komerční certifikáty, nikoli certifikáty kvalifikované. Informační systém datových schránek druh certifikátu sám kontroluje a neumožní uživateli zaregistrovat jiný než aktuálně platný komerční certifikát (viz obrázek 8-15).

Stejně tak si připomeňme, že jakmile je uživatelský certifikát zaregistrován, je již možné pouze přihlašování s tímto certifikátem (a nikoli bez něj, jen pomocí jména a hesla). Pokud se uživatel přesto pokusí o přihlášení jen pomocí jména a hesla, informační systém datových schránek mu to neumožní a dá mu najevo, že má zaregistrován uživatelský certifikát a že přihlášení je možné jen s ním.

Řekne to ale až po zadání jména a hesla, viz obrázek 8-16.[10]

[10] Jinak totiž systém nepozná, ke kterému účtu se uživatel přihlašuje, a tudíž nemůže poznat, zda je k tomu třeba certifikát.

Obrázek 8-15
Výběr uživatelského certifikátu pro přihlašování k datovým schránkám



Pokud se uživatel přihlašuje pomocí certifikátu, pak musí tento certifikát „ukázat“ ještě před tím, než bude zadávat své uživatelské jméno a heslo. Certifikát je po něm totiž požadován ihned, jakmile na přihlašovací obrazovce klikne na záložku „Certifikát“, viz následující obrázek.

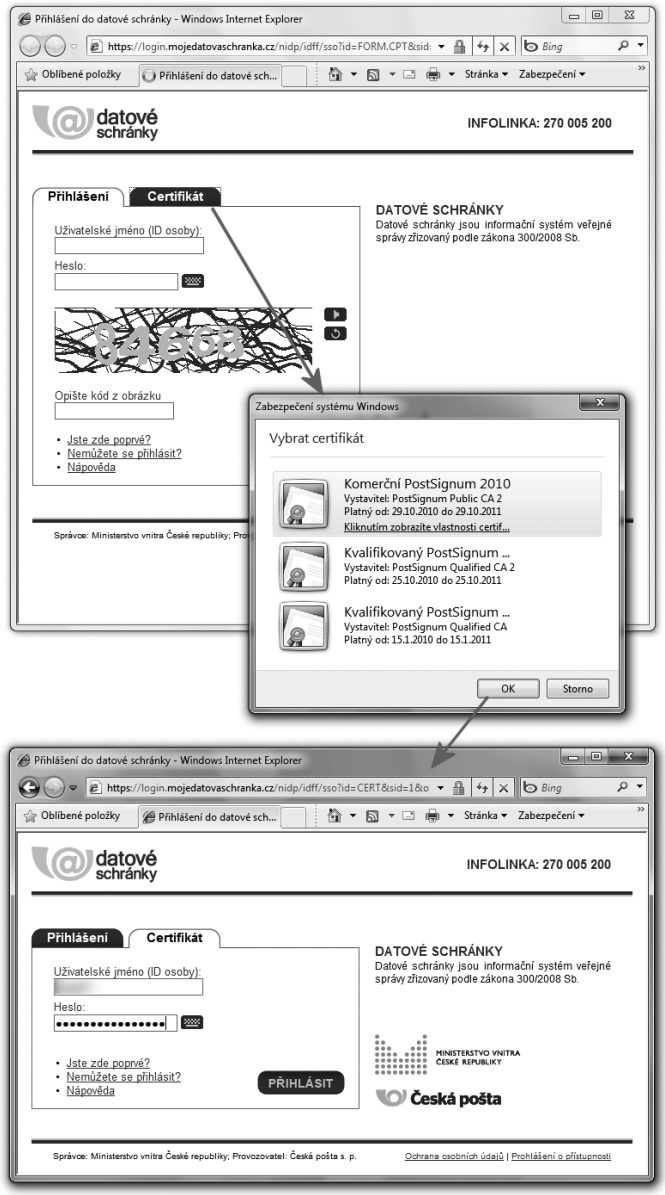
Obrázek 8-16
Upozornění na možnost přihlášení jen s certifikátem

Teprve po výběru certifikátu uživatel zadává své uživatelské jméno a heslo. Na rozdíl od přihlašování bez certifikátu nyní již nemusí vyplňovat tzv. captchu (ochranu proti robotům).

Pokud je vše v pořádku (byl vybrán správný certifikát a zadáno správné jméno a heslo), je uživatel řádně přihlášen a může se svou datovou schránkou pracovat.

Pokud ale něco není v pořádku, uživatel se dozví jen to, že došlo k nějakému problému, ale již se nedozví k jakému. Zda například zadal špatné jméno či heslo, nebo vybral nesprávný certifikát. Případně zda se pokouší přihlásit pomocí certifikátu, ale tato možnost pro něj není dostupná – nejspíše proto, že si žádný svůj uživatelský certifikát u informačního systému datových schránek nezaregistroval.

Obrázek 8-17
Přihlášení k datové schránce pomocí certifikátu



8.3 Zabezpečená komunikace

Dnešní celosvětový Internet, stejně jako většina dalších veřejných počítačových sítí, je ve své podstatě nezabezpečeným přenosovým mechanismem, a to v tom smyslu, že sám nedělá nic pro to, aby chránil přenášená data, zejména pokud jde o jejich důvěrnost. Konkrétně to znamená, že přenášená data nijak nešifruje, ale přenáší je „tak, jak jsou“.[11]

Stejně tak je celý dnešní Internet poměrně „důvěřivý“ i v tom smyslu, že předpokládá čestné a poctivé chování všech svých uživatelů i jejich aplikací. Vzhledem k tomu nemají jeho přenosové protokoly v sobě zabudovány prakticky žádné mechanismy, zvyšující bezpečnost například vůči tomu, kdy by se někdo chtěl vydávat za někoho, kým ve skutečnosti není.

Naštěstí ale Internet nijak nebrání tomu, aby si nezbytná opatření na zvýšení bezpečnosti zajistili sami uživatelé prostřednictvím svých aplikací a aplikačních protokolů, a díky tomu mohli bezpečně komunikovat i skrze tak málo bezpečné prostředí, jakým je dnešní Internet. Jen díky tomu můžeme dnes například platit on-line, ovládat svůj bankovní účet po Internetu (v rámci služeb internetbankingu) či třeba pracovat se svou datovou schránkou.

8.3.1 Sítě VPN

Ilustrativním příkladem toho, jak je možné vše vyřešit, jsou tzv. **privátní virtuální sítě**. Zkratkou **VPN**, z anglického **Virtual Private Network**.

Jde o řešení, které se chová jako skutečně privátní síť, nad kterou má její majitel plnou kontrolu a kterou má jen a jen pro sebe, resp. pro „své“ uživatele. A to včetně toho, že tato síť je zcela oddělena od všech ostatních sítí. Takže to, co se skrze ni přenáší, je nedostupné pro kohokoli, kdo k dané síti nemá přístup. A přístup může získat jen ten, komu jej zřídí majitel privátní sítě.

Pokud by ale takováto privátní síť měla být „skutečně privátní“ v tom smyslu, že by využívala svou vlastní přenosovou infrastrukturu,[12] pak by její pořízení a provozování bylo pro většinu zájemců nejspíše příliš drahé a také příliš náročné na správu, údržbu atd.

Aby tomu tak nebylo, zřizují se takovéto privátní sítě nikoli jako skutečné (skutečně privátní), ale pouze jako virtuální (ve smyslu virtuálně privátní). Fakticky jako nadstavba nad jinou sítí – třeba rovnou nad veřejným Internetem – která se pouze chová jako skutečně samostatná (a díky tomu i privátní) síť.

V nejjednodušším případě si takovou virtuální privátní síť (lidově VPN-ku) můžeme představit jako jakýsi tunel mezi dvěma body či uživateli, vedoucí skrze veřejný Internet a zprostředkovávající

---

[11] Výhodou tohoto přístupu je možnost udržet přenosové mechanismy jednoduché a efektivní – oproti stavu, kdyby se musely starat o zajištění důvěrnosti.

[12] Včetně přenosových cest a aktivních prvků, jako například směrovačů (router-ů).

zabezpečenou komunikaci těchto dvou stran: nikdo jiný se nedostane k tomu, co je mezi těmito dvěma stranami přenášeno. V obecnějším případě propojuje takovýto tunel více bodů či uživatelů, ale princip je stále stejný: nikdo jiný se nedostane k tomu, co je skrze tunel (resp. síť VPN) přenášeno, a stejně tak se nikdo (bez aktivního souhlasu majitele) nemůže k síti VPN připojit.

Snad každá virtuální privátní síť (síť VPN) využívá nějakou formu šifrování – k dosažení toho, aby se přenášený obsah nedostal do rukou někoho nepovolaného. Stejně tak vyžaduje vhodnou formu identifikace a autentizace toho, kdo se chce k síti VPN připojit. Záleží ale již na konkrétní implementaci, zda je k autentizaci využíván certifikát, nebo jen jméno a heslo, případně něco jiného.

8.3.2 SSL komunikace

Velmi podobnému účelu, a to zabezpečené komunikaci mezi dvěma stranami, slouží i řešení, které si můžeme označit jako **SSL komunikaci**. Specifikem je ale to, že jde o asymetrickou komunikaci mezi jednou stranou, která vystupuje jako **server**, a druhou stranou, která vystupuje jako **klient**.

Ačkoli jde o univerzální řešení, které mohou využívat různé aplikační protokoly, nejčastěji se s ním setkáme ve spojitosti s webem, neboli se službou World Wide Web. Serverem je pak webový server a klientem webový prohlížeč, resp. prohlížeč. Stejně tak by se ale mohlo jednat například o poštovní server a poštovního klienta či o FTP server a FTP klienta atd.

To, co SSL komunikacenabízí, jsou obecně tři různé přínosy:

- autentizace serveru vůči klientovi (aby klient měl jistotu, že komunikuje s tím, s kým si myslí, že komunikuje)
- identifikace klienta vůči serveru (aby si mohl být jist server)
- šifrování komunikace mezi klientem a serverem.

V praxi ale mohou být (a obvykle jsou) využívány jen dva přínosy, resp. cíle: autentizace serveru vůči klientovi a šifrování komunikace mezi klientem a serverem. Autentizace klienta vůči serveru je volitelná, protože mnohdy nemusí být ani potřebná. Nebo spíše: identifikace a autentizace klienta je často řešena jinak – a to samostatně, nikoli jako přímá součást SSL komunikace.

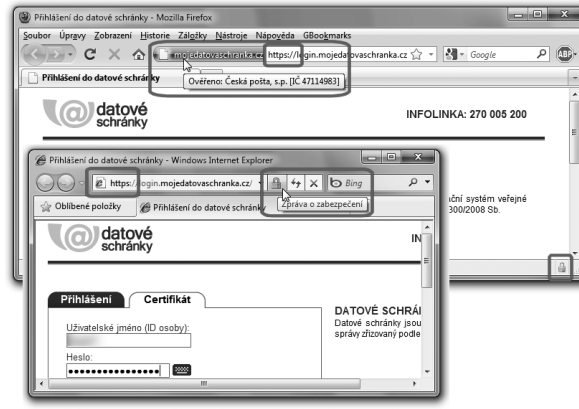
Obvykle je to tak, že nejprve je navázána zabezpečená komunikace mezi klientem a serverem na bázi SSL, v rámci které se server autentizuje vůči klientovi (a veškerá jejich vzájemná komunikace je nadále šifrována). Teprve následně, když již mezi oběma stranami existuje možnost zabezpečené komunikace, dochází k autentizaci klienta vůči serveru. Přesněji na straně klienta se autentizuje konkrétní uživatel – a to vůči konkrétní aplikaci, která běží na daném serveru.

Z této představy vycházely i příklady přihlašování, které jsme si popisovali v části 8.2. Všechny měly společné to, že by měly být používány až poté, co bylo mezi oběma stranami navázáno zabezpečené spojení prostřednictvím SSL komunikace.

To, že takovéto zabezpečené spojení mezi klientem a serverem existuje, pozná uživatel webového prohlížeče podle několika příznaků. Jedním z nich je jméno protokolu v URL odkazu na server: již nejde o (nezabezpečený) protokol HTTP, díky kterému URL odkazy začínají na **http://**. Nyní již jde o zabezpečený protokol HTTPS, kvůli němuž příslušná URL začínají na **https://**.

Vedle toho různé webové prohlížeče indikují existenci zabezpečené SSL komunikace i dalším způsobem, například ikonkou v podobě visacího zámku: Internet Explorer jej zobrazuje v adresovém řádku vpravo od URL odkazu, Firefox zase vpravo dole. Firefox pak přidává ještě grafické zvýraznění adresy serveru uvnitř adresového řádku, vlevo od URL odkazu, viz následující obrázek.

Obrázek 8-18
Indikace zabezpečeného SSL spojení s webovým serverem



Kliknutím na příslušný indikátor pak lze získat detailnější informace o certifikátu, kterým se server autentizuje. V případě Internet Exploreru je to ikonka visacího zámku, v případě Firefoxu barevně zvýrazněná doména vlevo od URL odkazu, viz obrázek na následující stránce.

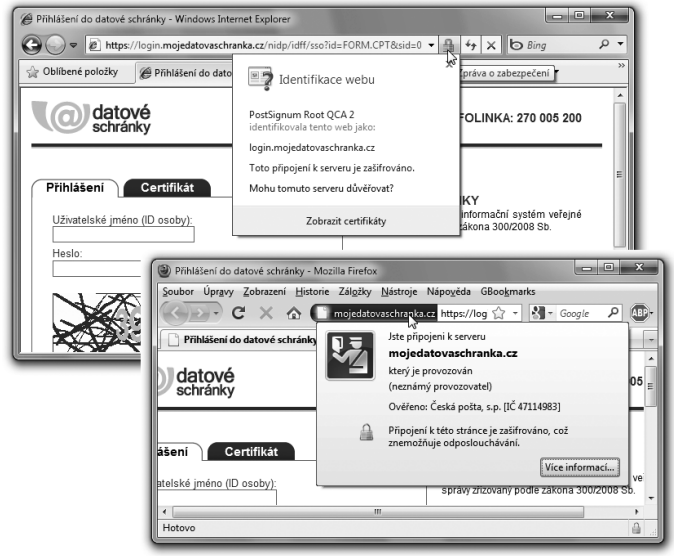
Zabezpečené SSL spojení mezi klientem a serverem přitom vzniká následujícím postupem:

- klient nejprve pošle serveru výzvu k navázání SSL spojení a domluví se na detailech tohoto spojení[13]
- server poskytne klientovi svůj (serverový) certifikát. Klient vyhodnotí jeho platnost a dále pokračuje jen tehdy, pokud tento certifikát shledá platným
- klient vygeneruje dočasný tajný klíč, který zašifruje veřejným klíčem serveru (ten získal z jeho certifikátu), a takto zašifrovaný klíč pošle serveru. Pokud je požadována i autentizace klienta (což obvykle není), připojí klient k zašifrovanému klíči i svůj certifikát[14]
- klient i server využijí dočasného tajného klíče k vygenerování „řádného“ tajného klíče, kterým pak šifrují svou vzájemnou komunikaci.

13 Například na tom, jaké kryptografické algoritmy budou společně používat.

14 Spíše ale certifikát uživatele, který klientský program právě používá.

Obrázek 8-19
Detailnější informace o serverovém certifikátu



Z pohledu koncového uživatele je většina těchto kroků neviditelná – až na dvě výjimky. Jednou z nich je (v praxi spíše výjimečný) požadavek na autentizaci klienta ještě v rámci navazování SSL spojení. V takovém případě je uživatel svým prohlížečem vyzván k výběru toho svého certifikátu, kterým se hodlá vůči serveru autentizovat.

Druhou výjimkou, která se obecně týká každého uživatele, je vyhodnocení platnosti certifikátu serveru.[15] To probíhá standardním způsobem, který jsme si popisovali v kapitole 3, a tedy i s posouzením důvěryhodnosti tohoto certifikátu – oproti obsahu toho úložiště, se kterým pracuje právě používaný prohlížeč.

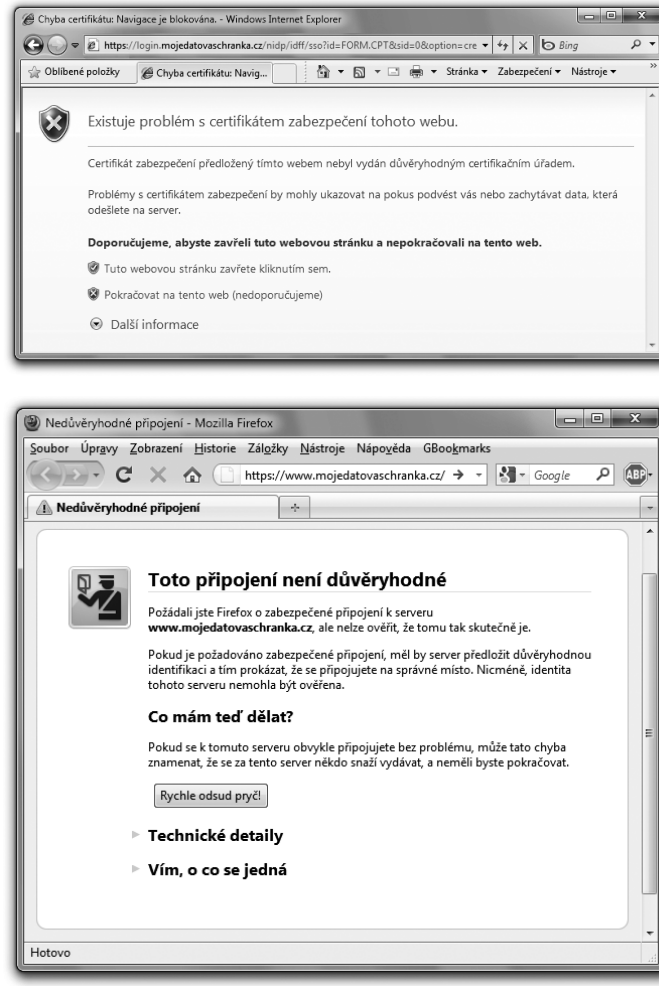
Právě zde ale může nastat nepříjemný problém: ačkoli může být certifikát serveru jinak „zcela v pořádku“, prohlížeč nemusí mít dostatečné informace k tomu, aby jej mohl prohlásit za důvěryhodný. Nejspíše proto, že „nezná“ tu certifikační autoritu, která jej vydala (neboť nemá její kořenový certifikát ve svém úložišti důvěryhodných kořenových certifikátů).

Stejně tak ale většinou nemá důvod považovat certifikát za nedůvěryhodný. Ve smyslu toho, co jsme si popisovali v kapitole 3, pak prohlížeč musí konstatovat „nevím“, neboli že nedokáže posoudit důvěryhodnost toho certifikátu, kterým se server prokazuje.

V praxi tato situace může nastávat častěji, než by si kdo přál, a to kvůli problému s počáteční náplní úložišť důvěryhodných certifikátů a s aktualizací této náplně. Viz podrobnější diskuse celého problému v 5. kapitole, v částech 5.4.3 a 5.4.4.

[15] Jde o systémový certifikát, kterému se obvykle říká „SSL certifikát“ či „serverový certifikát“.

> V ČR potkal tento problém datové schránky: server, na kterém běžel webový portál datových schránek, se prokazoval serverovým certifikátem, který mu vydala certifikační autorita PostSignum. Její kořenový certifikát ale nebyl součástí počáteční náplně snad žádného z používaných webových prohlížečů, a ani do nich nebyl automaticky načítán. A tak prohlížeče, používané prvními uživateli datových schránek, zcela správně dospěly k závěru, že o důvěryhodnosti příslušného serveru nemají dostatek informací.



Obrázek 8-20
Hlášky webových prohlížečů, když nemají dostatek informací k hodnocení důvěryhodnosti serverových certifikátů

Jak se ale má zachovat webový prohlížeč v situaci, kdy by měl navázat zabezpečené SSL spojení s konkrétním serverem, ale není schopen vyhodnotit jeho certifikát jako důvěryhodný? A když současně nemá žádný důvod, kvůli kterému by jej mohl považovat za nedůvěryhodný?[16]

Zřejmě jediným možným řešením je sdělit vše uživateli a nechat na něm, jak rozhodne.

Určitý problém je ale v tom, jakým způsobem to webové prohlížeče svým uživatelům sdělují. Většinou totiž uživateli naznačují spíše to, že příslušný server je nedůvěryhodný – a nikoli že o jeho důvěryhodnosti nemají dostatek informací.

Běžný uživatel si pak nemusí správně domyslet, kde je skutečná podstata problému – že vůbec nemusí být v nedůvěryhodnosti serveru, ale že může být i v nastavení jeho prohlížeče a jím používaného úložiště důvěryhodných certifikátů.

8.3.2.1 SSL certifikáty s rozšířenou validací (EV certifikáty)

V souvislosti se zabezpečenou komunikací mezi (webovými) servery a jejich klienty si ještě řekněme o tom, že může existovat více různých druhů SSL certifikátů, které identifikují konkrétní server. Mezi sebou se liší především tím, jak moc a jak důkladně je při jejich vydávání zkoumána identita žadatele a „identita“ serveru, který se bude tímto certifikátem prokazovat.

Certifikáty, kterými se prokazují webové servery a které slouží potřebám vedení SSL relací, jsou obecně komerčními certifikáty (nikoli kvalifikovanými certifikáty). Certifikační autority, které je vydávají, tak mají více prostoru k tomu, aby si individuálně přizpůsobily způsob a „důkladnost“ ověřování identity toho, kdo o takový certifikát žádá. Včetně ověřování údajů o samotném serveru, který se má certifikátem identifikovat.

Může se tak stát například i to, že serverový SSL certifikát bude vydán (jednoznačně a dostatečně) identifikovanému žadateli – ale certifikační autorita si již nebude vůbec ověřovat, zda dotyčný žadatel má možnost (a právo) provozovat server na adrese, která bude v serverovém certifikátu uvedena.

Proto mezi lety 2005 až 2007 vznikla v rámci privátního sektoru iniciativa, sdružující provozovatele certifikačních autorit a výrobci webových prohlížečů, s cílem definovat přísnější požadavky na vydávání serverových SSL certifikátů. Tyto požadavky se týkají jak identifikace samotného žadatele o vydání certifikátu (který se mj. musí dostavit osobně na certifikační autoritu), tak i jeho práva provozovat server na zadané doméně druhého řádu.[17]

---

16 Například kvůli revokaci příslušného certifikátu, případně kvůli zařazení tohoto certifikátu či certifikátu jeho vydavatele mezi nedůvěryhodné (v systémovém úložišti MS Windows).

17 Toto se ověřuje jednak u registrátora příslušné domény, ale také v rámci služby WHOIS.

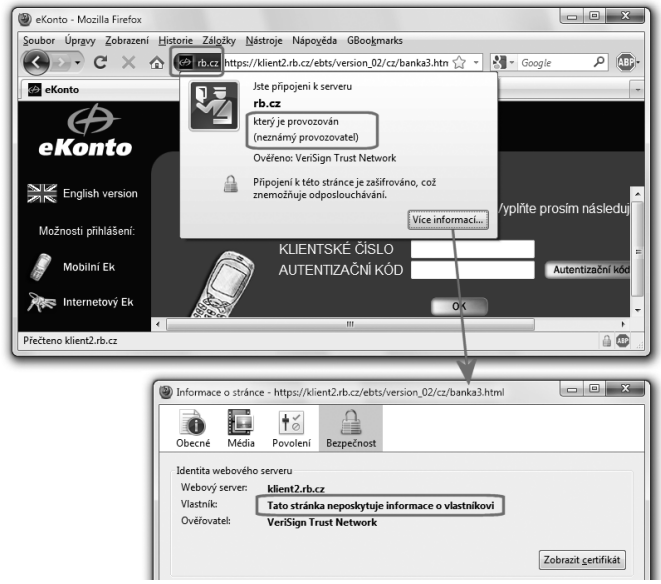
Ty certifikáty, které jsou vydány za splnění takto zpřísněných podmínek, pak jsou označovány jako **certifikáty s rozšířenou validací** (**EV certifikáty**, z anglického: **Extended Validation**). Touto „rozšířenou validací“ je přitom myšleno právě (a pouze) zpřísnění podmínek při vydávání certifikátu, pokud jde o ověření (validaci) žadatele a jeho práva provozovat server na zadané doménové adrese. Jinak, například co do síly kryptografických algoritmů či velikosti klíčů, se takovéto EV certifikáty nijak neliší od „běžných“ serverových SSL certifikátů (pro odlišení někdy označovaných také jako „basic“).

Vzhledem k tomu, že se na celé iniciativě podíleli i výrobci webových prohlížečů,[18] mohou být její výsledky přímo „integrovány“ do jejich produktů. Jinými slovy: některé dnešní prohlížeče (nikoli ale všechny) dokáží rozpoznat serverové certifikáty s rozšířenou validací a pracovat s nimi odlišně od „běžných“ (basic) serverových certifikátů.

Konkrétním projevem může být to, jaké informace prohlížeč zobrazuje v závislosti na druhu serverového certifikátu. Jde-li pouze o certifikát „Basic“, pak prohlížeč podporující EV certifikáty raději nezobrazuje identitu držitele certifikátu coby provozovatele serveru. Jako kdyby neměl dostatečnou jistotu, že by to odpovídalo pravdě.

Příklad ukazuje následující obrázek, který lze srovnat i s předchozími obrázky: je na něm přístup k serveru, který se prokazuje pouze „základním“ (basic) serverovým SSL certifikátem, a nikoli EV certifikátem.

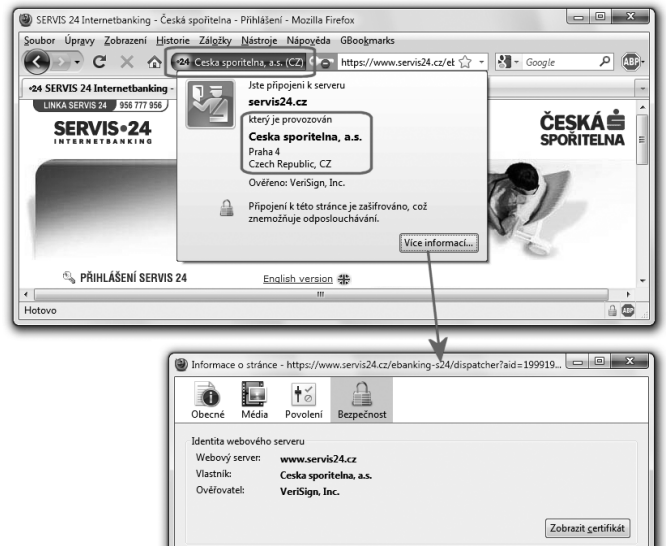
Obrázek 8-21
Příklad serveru, který se prokazuje pouze základním (Basic) serverovým SSL certifikátem



18 Náš právní řád ale takovéto druhy komerčních certifikátů nezná, a tuzemské certifikační autority je nevydávají.

Další obrázek již ukazuje příklad serveru, který se prokazuje EV certifikátem. Zde již jsou údaje o provozovateli serveru řádně uvedeny – a příslušná část adresového řádku je pro odlišení zbarvena do zelena.

Obrázek 8-22
Příklad serveru, který se prokazuje serverovým certifikátem s prodlouženou validací (EV certifikátem)



8.3.3 DNSSEC

Poslední příklad zabezpečené komunikace, který si zde popíšeme, se týká fungování systému DNS (Domain Name System). Ten má v rámci Internetu na starosti překlad symbolických doménových jmen na číselné IP adresy, ale je dnes využíván i k řadě dalších účelů.

Komunikace v rámci systému DNS, mezi jeho klienty (resolvery) a servery (name servery), ale není nijak zabezpečena – což otevírá prostor pro případné útoky, vedené cestou narušení či přímo podvržení této komunikace.

> Příkladem může být phishing, při kterém se útočník snaží podstrčit své oběti falešné stránky (například jeho banky apod.) a snaží se jej přimět k tomu, aby těmto falešným stránkám zadal své údaje (přihlašovací údaje či rovnou údaje o svých platebních kartách apod.).

Jednou z možností, jak phishing realizovat, je nechat uživatele kliknout na (či přímo zadat) nějakou „podobně vypadající“ URL adresu, na které se pak nachází falešné stránky. Pozornější uživatel si ale může všimnout i drobné odlišnosti v symbolické (URL) adrese a pokus o podvod odhalit. Sofistikovanější phishingové (ale i jiné) útoky se proto pokouší napadnout mechanismus DNS, který překládá mezi symbolickými doménovými jmény a číselnými IP adresami,

a změnit jeho fungování. Pokud by se jim to podařilo, dopadlo by to tak, že uživatel zadá zcela správnou symbolickou (URL) adresu, ale ta je přeložena na nesprávnou (jinou) IP adresu, na které jsou pak umístěny podvodné stránky.

Samozřejmě ale existují i řešení, která fungování systému DNS zabezpečují a podobné útoky znemožňují. Zejména systém DNSSEC (DNS Security Extensions).

Princip fungování systému DNSSEC si lze představit tak, že veškerá komunikace v rámci systému DNS (mezi jeho servery) je elektronicky podepisována. Díky tomu může mít každá součást celého systému, která se na něco ptá jiné součásti – konkrétně třeba na převod mezi symbolickou (URL) adresou a odpovídající číselnou IP adresou – rozumnou jistotu, že dostala správnou odpověď, a nikoli nějakou podvrženou odpověď.

Celá věc má ale dva drobné háčky. Prvním je ten, že DNSSEC dosud nepoužívá zdaleka celý systém DNS, ale jsou jím zabezpečeny jen některé domény (resp. jejich name servery). Situace se sice neustále zlepšuje, s tím jak jsou další a další domény zabezpečovány pomocí DNSSECu – ale i přesto je nutné počítat s tím, že jen některé odpovědi generované systémem DNS jsou tímto způsobem zabezpečeny (ty, které se týkají dotazů na domény, využívající DNSSEC).

Při odpovídání na dotazy, týkající se konkrétních domén, tak mohou v rámci DNS nastat tři různé případy, které si rovnou očíslujme:

1. příslušná doména není zabezpečena pomocí DNSSEC (a odpověď na dotaz, týkající se této domény, tak ani nemůže být zabezpečena pomocí elektronického podpisu)
2. příslušná doména je zabezpečena pomocí DNSSEC a odpověď na dotaz ohledně této domény je platně podepsaná (neboť elektronický podpis na odpovědi byl ověřen jako platný)
3. příslušná doména je zabezpečena pomocí DNSSEC, ale odpověď na dotaz nemůže být považována za platnou (protože elektronický podpis na odpovědi nemohl být ověřen jako platný)

Druhý drobný háček je pak v tom, že DNSSEC skutečně zabezpečuje komunikaci jen v rámci systému DNS, mezi jeho jednotlivými servery (name servery, pokud DNSSEC podporují), a nikoli již komunikaci „směrem ven“, mezi koncovým uživatelem a „nejbližším“ DNS serverem, jehož služby tento koncový uživatel právě využívá.

Lze se na to dívat také tak, že DNSSEC zabezpečuje fungování celého systému DNS „zevnitř“, aniž by se měnil konkrétní způsob jeho fungování směrem ven, ke koncovým uživatelům. Ti tak mohou profitovat z přínosů DNSSEC (vyšší bezpečnosti), aniž by pro to museli sami cokoli dělat či měnit na své straně.

Jenže informace o důvěryhodnosti odpovědi (ve smyslu tří výše uvedených možností) by se hodila i koncovému uživateli. I on by ji mohl využít k tomu, aby se snáze vyvaroval některým potenciálním nástrahám a úskalím či přímo útokům. Jak ale požadované informace ze systému DNS dostat ven?

Určité řešení již existuje, byť je dostupné jen pro některé aplikace. Konkrétně pro prohlížeč Firefox, v podobě dodatečně instalovaného softwarového modulu (plug-in modulu), z dílen laboratoří CZ.NICu. Jmenuje se příznačně: DNSSEC validátor, a je ke stažení zdarma v rámci standardní nabídky doplňků a rozšíření prohlížeče Firefox, nebo přímo z jeho vlastních stránek, na adrese *http://dnssec-validator.cz*.

Obrázek 8-23
Nabídka DNSSEC validátoru pro prohlížeč Mozilla Firefox

Na následující trojici obrázků pak vidíte, jak tento modul indikuje tři výše popsané situace, týkající se dotazu na doménu, která není zabezpečena pomocí DNSSEC či která zabezpečena je (a dotaz je platně podepsán, nebo naopak platně podepsán není).

Obrázek 8-24
Indikace, že doména servis24.cz není zabezpečena pomocí DNSSEC

Obrázek 8-25
Doména mojedatovaschranka.cz je zabezpečena a poskytnuté údaje jsou platně podepsané

Obrázek 8-26
Doména nic.cz je zabezpečena ale poskytnuté údaje nejsou platně podepsané

Zastavme se podrobněji u třetí ukázky, příznačně symbolizované červeným klíčkem. Zde plug-in zjistil (v důsledku uměle navozené chyby), že podpis na odpovědi, týkající se domény nic.cz (jinak zabezpečené prostřednictvím DNSSEC) byl opatřen elektronickým podpisem, který ale nemohl být ověřen jako platný.

Toto zjištění může, ale také nemusí znamenat, že skutečně došlo k nějakému útoku a uživatel byl ve skutečnosti zaveden na jiné webové stránky, na podvržené IP adrese.

Plug-in DNSSEC validátor ale chrání uživatele ještě jiným způsobem, a to tím, že sám kontroluje správnost převodu symbolického doménového jména (jména domény) na číselnou IP adresu – a pokud i zde zjistí nějakou odlišnost, upozorní na to uživatele.

Takovouto situaci lze vidět na obrázku na následující stránce. Je na něm příklad s URL adresou, zahrnující doménu *rhybar.cz*. Ta je provozována sdružením CZ.NIC pro demonstrační účely (jako právě zde), aby se na ní daly předvádět účinky zabezpečení pomocí DNSSEC. Je totiž záměrně „poškozena“, tak aby odpovědi na dotazy k této doméně vykazovaly neplatný podpis, a díky tomu mohla být uživateli „podstrkována“ jiná IP adresa, než jaká by správně měla. Všimněte si proto poněkud odlišné hlášky DNSSEC validátoru v tomto případě, kdy upozorňuje i na pravděpodobné podvržení IP adresy.

Pro správné a plnohodnotné fungování DNSSEC validátoru na počítači uživatele ale musí být splněna jedna důležitá podmínka: sám tento validátor musí komunikovat se systémem DNS prostřednictvím takového DNS serveru, který podporuje DNSSEC a je dostatečně důvěryhodný.

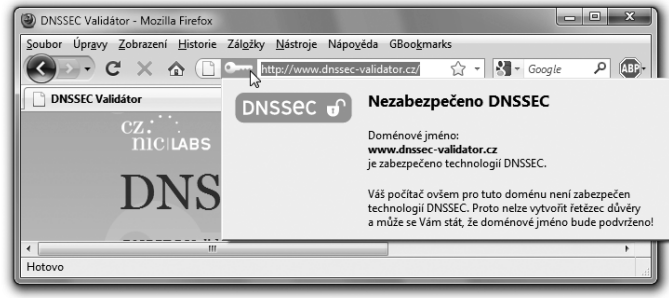
Obrázek 8-27
Signalizace neplatného podpisu a pravděpodobně podvržené IP adresy

> Nezapomínejme na požadavek důvěryhodnosti DNS serveru: pokud by tento DNS server byl napaden útočníkem, mohl by uvést v omyl i DNSSEC validátor, který by pak hlásil „vše v pořádku“ i tam, kde by to v pořádku nebylo.

Samotný DNSSEC validátor pochopitelně dokáže rozpoznat, když je nucen komunikovat s takovým serverem, který sám DNSSEC nepodporuje. Potom se dokáže vyjádřit jen k tomu, zda příslušná doména jako taková je zabezpečena pomocí DNSSEC, ale již nedokáže vyhodnocovat správnost jednotlivých odpovědí na dotazy (skrze platnost podpisu na nich).

Způsob, jakým DNSSEC validátor tuto situaci signalizuje, vidíte na následujícím obrázku.

Obrázek 8-28
DNSSEC validátor signalizuje, že doména je zabezpečena pomocí DNSSEC, ale on nedokáže hodnotit jednotlivé odpovědi



Čím je ale určeno to, s jakým DNS serverem validátor právě spolupracuje a skrze něj i vyhodnocuje platnost odpovědí?

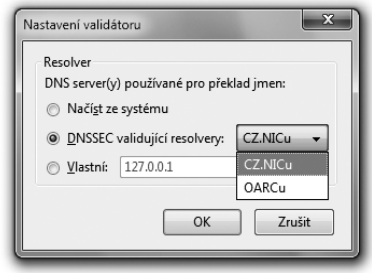
To záleží na jeho nastavení, kde mu lze použité DNS servery předepsat. Možnosti jsou následující:[19]

[19] Ve Firefoxu je najdeme přes správce doplňků v Možnostech příslušného plug-inu.

- „načíst ze systému“: zde DNSSEC validátor bude pracovat s těmi samými DNS servery, jako operační systém počítače, na kterém prohlížeč běží. Ty mohou, ale také nemusí DNSSEC podporovat
- „DNSSEC validující resolvery“: zde lze zvolit servery (resolvery), které provozuje sdružení CZ.NIC (nebo organizace OARC), a které DNSSEC podporují
- „vlastní“: zde lze zadat konkrétní IP adresu DNS serveru, který má být používán. V úvahu připadá (například) vlastní DNS server, firemní DNS server s podporou DNSSEC atd.

Obrázek 8-29

Nastavení používaných DNS serverů



Aby DNSSEC validátor dokázal odhalit i podvržené IP adresy, je vhodné jej nastavit na druhou či třetí možnost (a nikoli na první) – protože pak dostává přeložené IP adresy ze dvou různých zdrojů a může je porovnávat.

Literatura a další zdroje

Literatura a další zdroje

Knižní publikace

D. Bosáková, A. Kučerová, J. Peca, P. Vondruška: Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů
Nakladatelství ANAG, 2002
ISBN 80-7263-125-X
Dostupné ke stažení on-line na: http://crypto-world.info/kniha/elektronicky_podpis.pdf

Petr Budiš: Elektronický podpis a jeho aplikace v praxi
Nakladatelství ANAG, 2008
ISBN 978-80-7263-465-1

Libor Dostálek, Marta Vohnoutová: Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, 2. aktualizované vydání
Nakladatelství Computer Press, leden 2010
ISBN 978-80-251-2619-6

Dozorový orgán

Ministerstvo vnitra ČR, Odbor koncepce a koordinace ICT ve veřejné správě
www.mvcr.cz/clanek/odbor-koncepce-a-koordinace-informacnich-a-komunikacnich-technologii-ve-verejne-sprave-687897.aspx

MV ČR: Informace k používání elektronického podpisu
www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

MV ČR: Přehled udělených akreditací
www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx

Elektronický podpis pro komunikaci s orgány veřejné moci
Portál veřejné správy, postup řešení životní situace.
http://portal.gov.cz/wps/portal/_s.155/701/_s.155/708?uzel=7&POSTUP_ID=574

Akreditované certifikační autority

I.CA (První certifikační autorita, a.s.)
Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
www.ica.cz

PostSignum (Česká pošta, a.s.)
Olšanská 38/9, PSČ 225 99 Praha 3
www.postsignum.cz

eIdentity (eIdentity a.s.)
Vinohradská 184/2396, PSČ 130 00 Praha 3
www.eidentity.cz

Legislativa

Zákon č. 227/2000 Sb., o elektronickém podpisu
http://portal.gov.cz/wps/portal/_s.155/701?number1=227%2F2000

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
http://portal.gov.cz/wps/portal/_s.155/701?number1=300%2F2008

Zákon č. 499/2004 Sb., o archivnictví a spisové službě
http://portal.gov.cz/wps/portal/_s.155/701?number1=499%2F2004

Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb
http://portal.gov.cz/wps/portal/_s.155/701?number1=378%2F2006

Vyhláška č. 495/2004 Sb., k provádění zákona o elektronickém podpisu
http://portal.gov.cz/wps/portal/_s.155/701?number1=495%2F2004

Vyhláška č. 496/2004 Sb., o elektronických podatelnách
http://portal.gov.cz/wps/portal/_s.155/701?number1=496%2F2004

On-line podpora knihy

On-line podpora knihy

Tato kniha popisuje problematiku elektronického podpisu tak, jak vypadala v roce 2010 (kdy kniha vznikala). Vývoj ale jde velmi rychle kupředu a některé popisované skutečnosti i souvislosti se postupem času mohou významněji měnit. Klasický knižní titul ale na takovýto vývoj může reagovat jen s určitým zpožděním, formou dalších (aktualizovaných) vydání.

V dnešní době, díky Internetu, ale existuje i jiná možnost: popsat příslušné změny a novinky on-line, na vhodných webových stránkách. Proto byla k této knize zřízena její webová podpora, na adrese **http://bajecnysvet.cz**.

Najdete zde nejenom aktuální informace o novinkách v oblasti elektronického podpisu a případných změnách v jeho legislativní úpravě, ale i další obsah, související s knihou. Například ukázkové příklady, na kterých si můžete sami vyzkoušet ověřování nejrůznějších variant podepsaných či označených elektronických dokumentů (ve formátu PDF či ve formátech MS Office).

Stejně tak zde najdete diskusní fórum k otázkám elektronického podpisu či nabídku kurzů elektronického podpisu, vedených autorem této knihy.

Jiří Peterka
BÁJEČNÝ SVĚT ELEKTRONICKÉHO PODPISU

www.bajecnysvet.cz

Vydavatel:
CZ.NIC, z. s. p. o.
Americká 23, 120 00 Praha 2
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2011
Kniha vyšla jako 4. publikace v Edici CZ.NIC.

ISBN 978-80-904248-3-8 (tištěná verze, PDF)

CZ NIC | SPRÁVCE DOMÉNY CZ

Edice CZ.NIC

Tato kniha je psána pro lidi, kteří chtějí (či musí) používat elektronický podpis, chtějí mu rozumět, ale současně nepotřebují být odborníky na kryptografii. Celou složitou problematiku elektronického podpisu vysvětluje autor na třech úrovních: na úrovni úvodu a celkového přehledu, na úrovni principů elektronického podpisu a na úrovni běžné praxe (příprava počítače, podpisy na PDF dokumentech, podpisy v rámci MS Office, šifrování, přihlašování a zabezpečená komunikace).

O autorovi **Jiří Peterka** přednáší počítačové sítě a komunikace na Matematicko-fyzikální fakultě UK v Praze. Současně působí jako nezávislý konzultant a publicista, který se věnuje problematice Internetu a informační společnosti. K elektronickému podpisu se poprvé dostal v roce 1999, kdy vznikal zákon o elektronickém podpisu. Byl členem pracovní skupiny, která připravovala finální znění tohoto zákona. K problematice elektronických podpisů se znovu dostal o deset let později, v souvislosti se spuštěním datových schránek a celkovou elektronizací v oblasti eGovernmentu.

O edici Edice CZ.NIC je jedním z osvětových projektů správce české domény nejvyšší úrovně. Cílem tohoto projektu je vydávat odborné, ale i populární publikace spojené s internetem a jeho technologiemi. Kromě tištěných verzí vychází v této edici současně i elektronická podoba knih. Ty je možné najít na stránkách knihy.nic.cz

ISBN 978-80-904248-3-8

knihy.nic.cz