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".

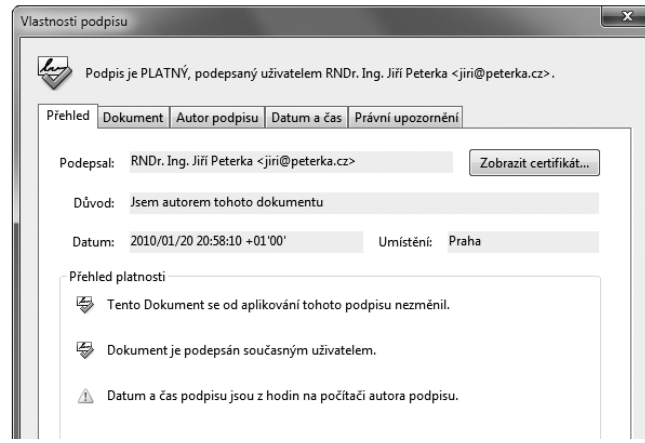
Pokud bychom (jakýkoli) vlastnoruční podpis dali ke zkoumání grafologovi, zabýval by se tím, jak je veden tah perem, jaký je sklon a tvar jednotlivých znaků, případně jaký inkoust byl při jeho tvorbě použit, na jakém papíře se podpis nachází atd.

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]

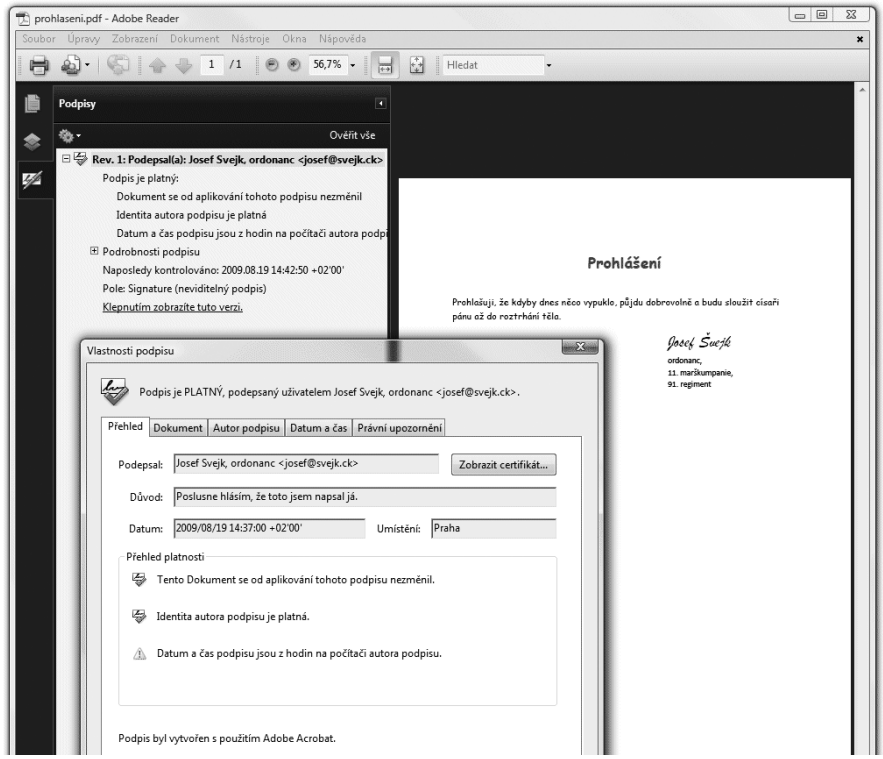
K tomu, abychom se mohli spolehnout na identitu podepsané osoby, nám tedy „pouhý“ zaručený elektronický podpis nestačí. K tomu již potřebujeme uznávaný elektronický podpis (zmiňovaný v předchozím odstavci), který je v tomto ohledu „silnější“. Na rozdíl od zaručeného elektronického podpisu klade přísné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

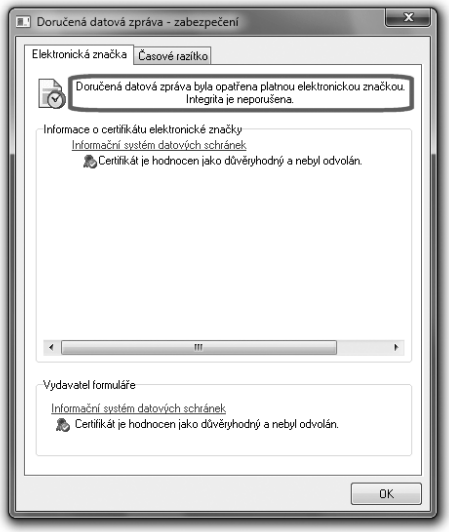
Elektronický podpis má ještě jeden zajímavý aspekt: je určen pouze lidem, resp. fyzickým osobám. Neexistuje žádný elektronický podpis právnické osoby, organizace, úřadu apod. Je to vlastně stejné jako u vlastnoručních podpisů: podepsat se (elektronicky) může jen fyzická osoba, která právě jedná jménem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

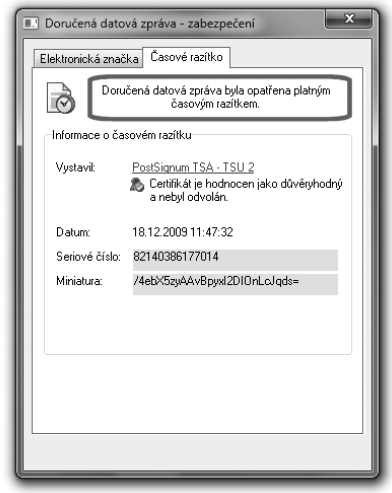
Praxe si nicméně vynutila obdobu elektronického podpisu, která již je dostupná i jiným subjektům, než jen fyzickým osobám. Konkrétně právnickým osobám (firmám, organizacím atd.), i organizačním složkám státu. Jde o tzv. **elektronickou značku**: ta je po technické stránce (zaručeným) elektronickým podpisem, 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.

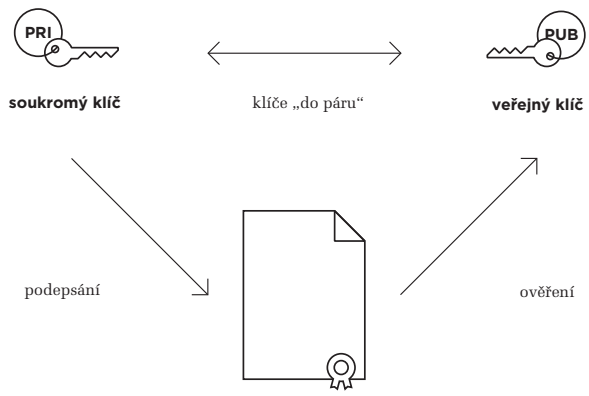
Důvodem je to, že právě soukromý klíč je tím, co potřebujeme pro vytváření vlastního elektronického podpisu. Je to „to", co nás jednoznačně identifikuje – a pokud bychom "to" (tedy náš soukromý klíč) dali někomu jinému, mohl by se podepisovat naším jménem. To jistě nechceme, a tak si musíme svůj soukromý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

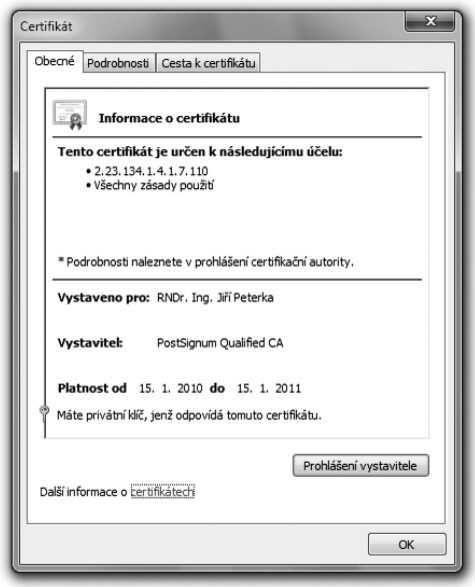
Řešení naštěstí není principiálně složité: stačí najít někoho třetího – nějakou dostatečně důvěryhodnou autoritu – která potvrdí, komu veřejný klíč patří. A aby to nemusela deklarovat pokaždé znovu, vystaví na to jakési opakovaně využitelné potvrzení, které také sama podepíše (opatří vlastním elektronickým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

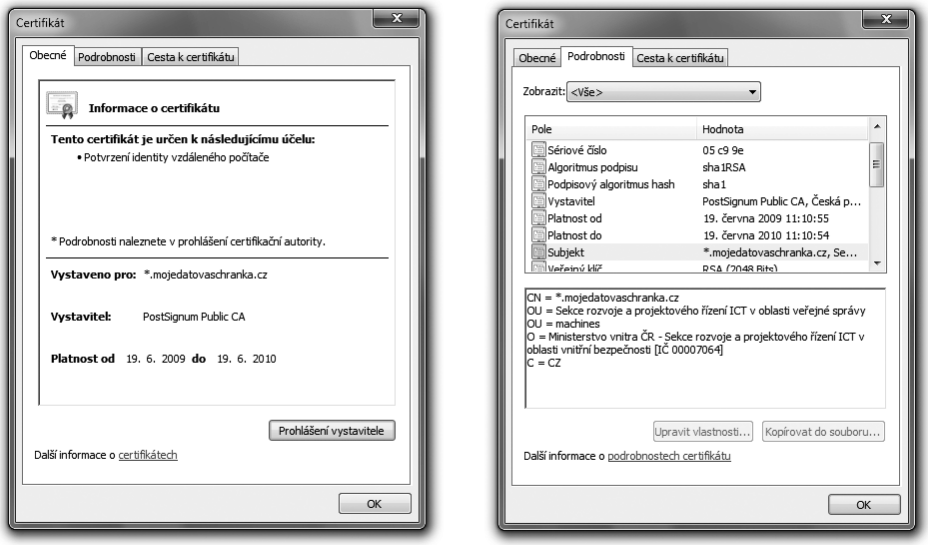
Zákony a nejrůznější vyhlášky ke stejnému sdělení používají ještě jinou formulaci, když hovoří o „*certifikátu, na kterém je elektronický podpis založen*“. Striktní dodržování tohoto slovního obratu ale leckdy komplikuje popis jinak jednoduchých a prostých skutečností nad hranici jejich srozumitelnosti.

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

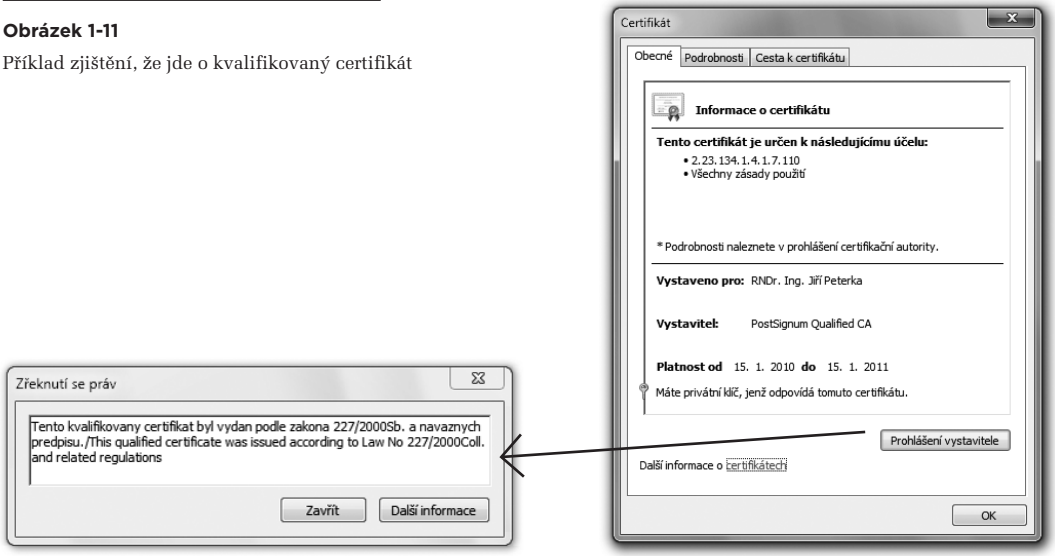
Příklad systémového certifikátu, který byl vystaven Ministerstvu vnitra, pro Informační systém datových schránek (ISDS), provozovaný na adrese mojedatovaschranka.cz



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.

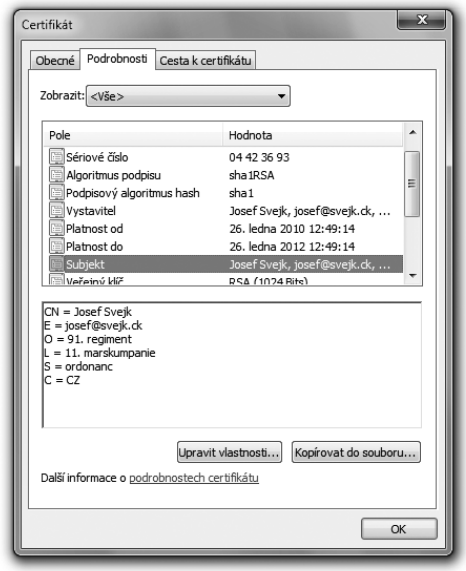
[12] Zákon ani nezná pojem „komerční certifikát“, v praxi se pod tento pojem zahrnují všechny certifikáty, které nejsou kvalifikované. Ale také ne vždy: někdy jsou například emailové certifikáty (či testovací certifikáty) chápány jako samostatné druhy certifikátů. Zde ale budeme vycházet z předpokladu,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

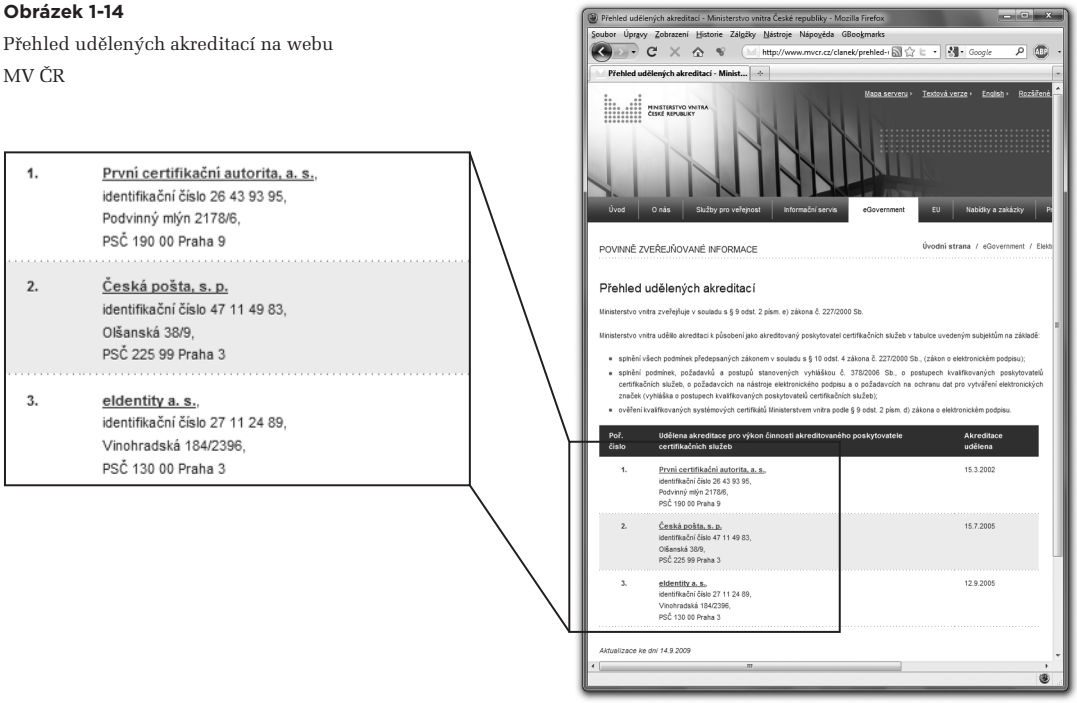
> Kvalifikované certifikáty mohou vydávat pouze takovéto kvalifikované certifikační autority. Komerční certifikáty již mohou vydávat všechny certifikační autority.

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.

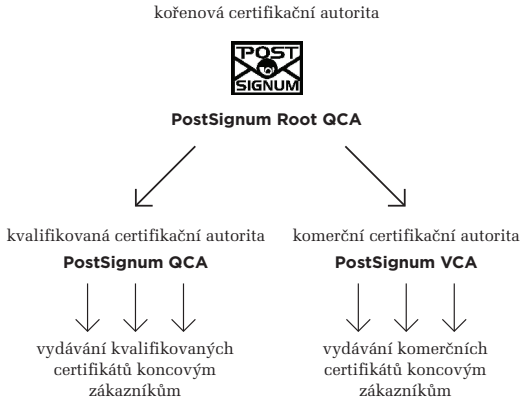
1.11.2 Kořenové a podřízené certifikační autority

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

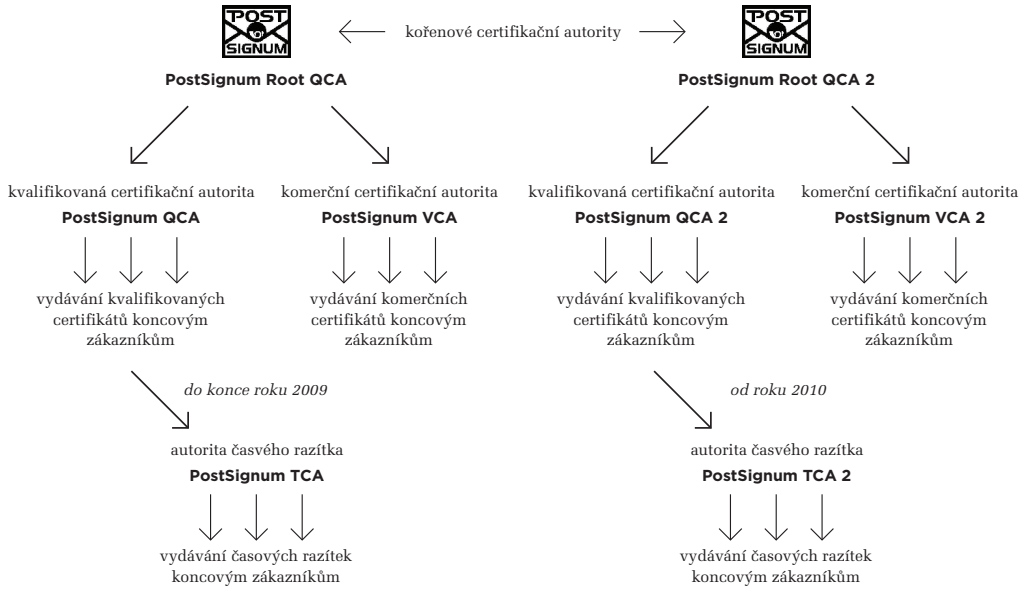


Počátkem roku 2010 pak, v souvislosti s přechodem na novou hašovací funkci SHA-2, svou vnitřní strukturu jakoby zdvojila: přidala novou kořenovou autoritu (PostSignum Root QCA 2), novou kvalifikovanou certifikační autoritu (PostSignum QCA 2, též PostSignum Qualified CA 2) a novou komerční certifikační 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

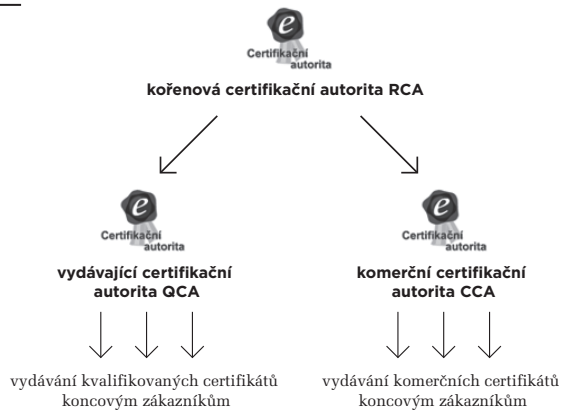


Hlavní rozdíl mezi původními a „dvojkovými“ autoritami PostSignum je přitom v tom, zda používají starší hašovací funkci SHA-1 (původní autority) nebo novou SHA-2 (nové „dvojkové“ autority).

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

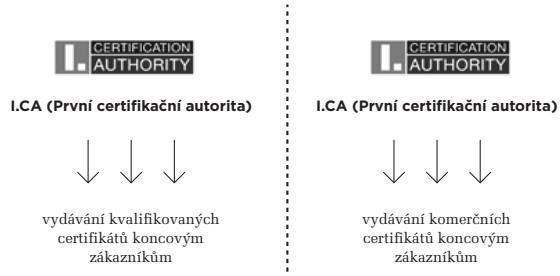
Obrázek 1-17

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.

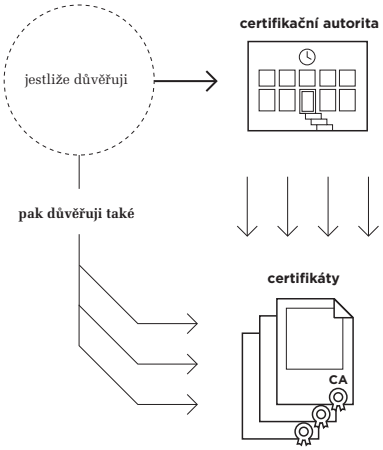
Důvěryhodnost každého certifikátu samozřejmě můžeme posuzovat individuálně, pro každý jednotlivý certifikát, a to na základě takových informací, jaké máme k dispozici. Třeba pokud nám někdo, koho dobře známe a v koho máme důvěru, sám předá konkrétní certifikát a prohlásí ho za svůj vlastní, asi můžeme 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.

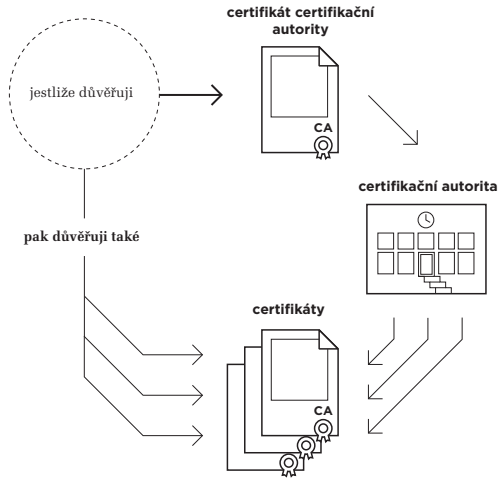
U certifikátů a certifikačních autorit navíc platí něco, co bychom mohli označit jako „delegaci důvěry“: když budu důvěřovat nějaké konkrétní certifikační autoritě, mohu důvěřovat i všem certifikátům, které tato certifikační autorita vydala. Což je jinými slovy totéž, jako tvrzení že důvěryhodnost konkrétního 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



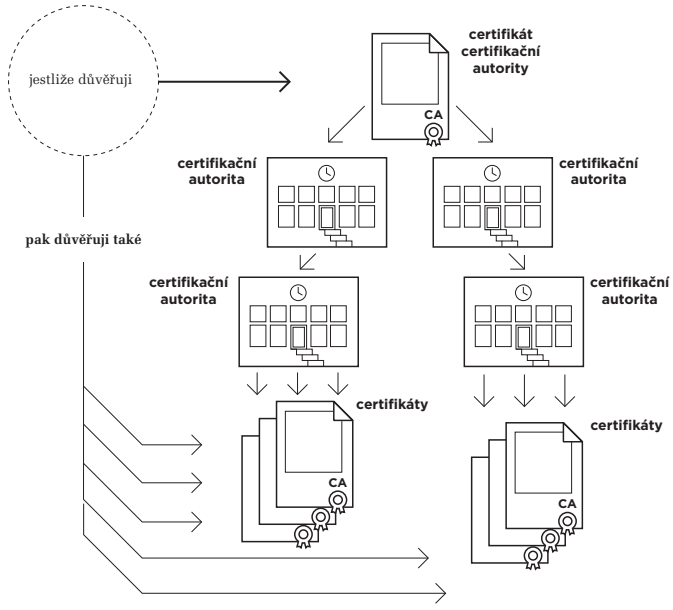
V praxi by ale nebylo příliš praktické vyjadřovat svou důvěru konkrétní certifikační autoritě „jako takové“. Nebylo by ani moc jasné, jak to vlastně udělat (po technické stránce). Naštěstí i zde existuje řešení, založené na tom, že i sama certifikační autorita používá k vydávání certifikátů nějaký vlastní 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

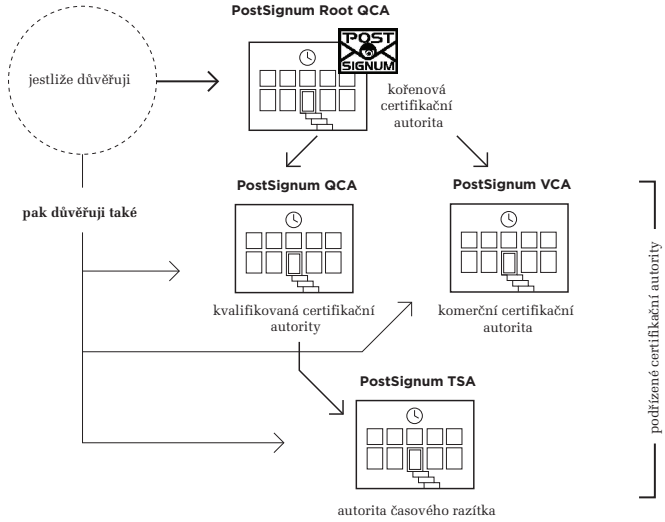


Vše se tedy dá zobecnit, do celého **stromu důvěry**: v jeho kořeni je jeden certifikát (tzv. **kořenový certifikát**), který odpovídá jedné (typicky: kořenové) certifikační autoritě. Od něj se odvíjí důvěra v další certifikáty (všechny vnitřní uzly stromu, tj. „podřízené“ certifikační autority, resp. 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

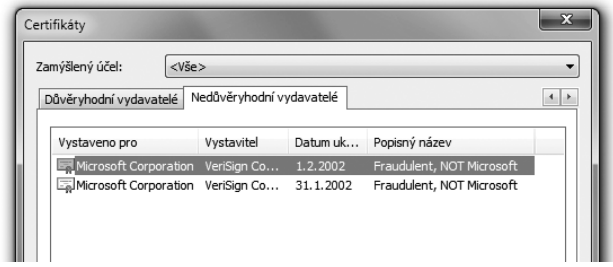
Konkrétní způsob, jakým „na svém počítači" vyjádříme důvěru konkrétnímu certifikátu, ať již kořenovému či jinému, je dán tím, jakým způsobem pracují s certifikáty nejrůznější programy: uchovávají si je ve speciálních **úložištích certifikátů** (anglicky **certificate store**).

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.

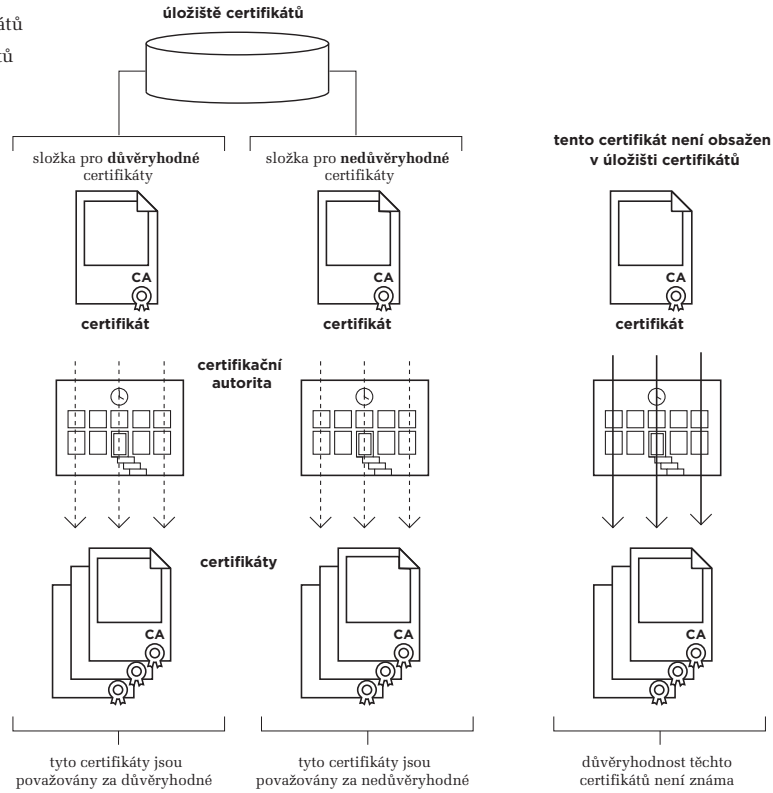
> Například programy z produkce Microsoftu používají systémové úložiště certifikátů, které vytváří operační systém MS Windows. Jiné programy, jako třeba Adobe Reader, Adobe Acrobat či prohlížeč Firefox, mají vlastní úložiště. Ale třeba právě Adobe Reader či Acrobat dokáží používat i systémové úložiště,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

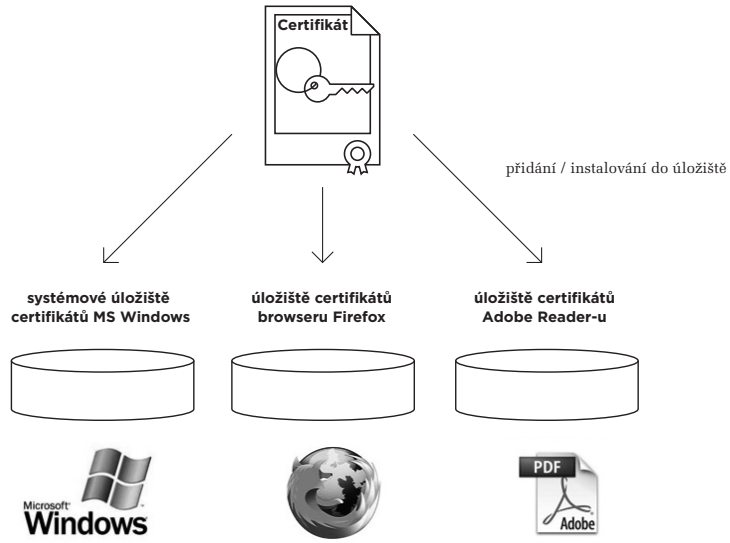
Nejčastěji v tom smyslu, že uživatel má důvod považovat za důvěryhodné i další certifikáty (resp. celé stromy certifikátů), ale ty „od výrobce“ v příslušném úložišti obsaženy nejsou. Pak je na něm, aby si je do úložiště přidal.

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

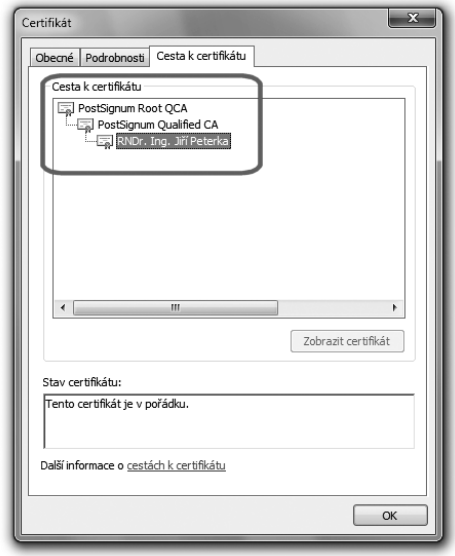
Aby výše popsaný princip vyjadřování důvěry mohl v praxi fungovat a důvěra v konkrétní certifikáty mohla být odvozována od jejich příslušnosti do konkrétního stromu důvěry, musí každý certifikát obsahovat určité minimální údaje, sloužící těmto účelům.

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]

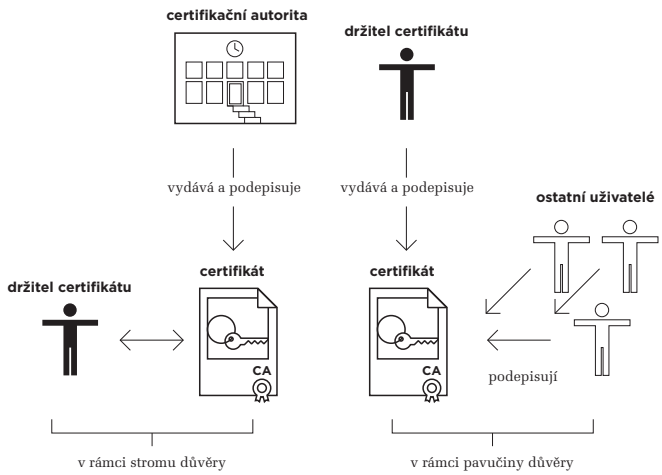
Jak je ale potom posuzována důvěryhodnost takovýchto certifikátů?

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



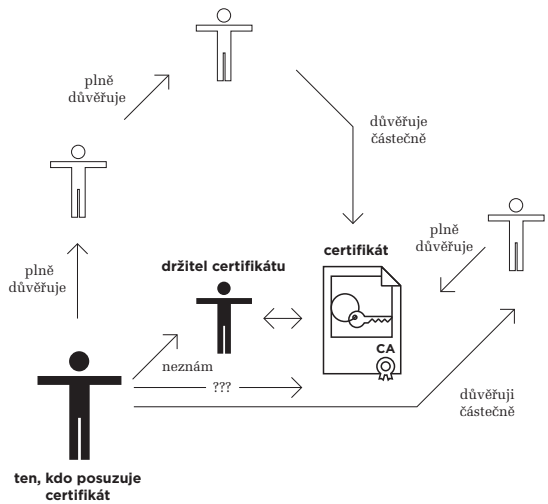
Jinými slovy: i zde je zásadní odlišnost oproti stromu důvěry, kde podpis certifikační autority na jí vydaném certifikátu má jen jeden možný význam (ve smyslu „plné důvěry"). Z pohledu toho, kdo s certifikátem pracuje, má pak důvěryhodnost absolutní charakter: certifikát pro něj buďto je důvěryhodný, 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.