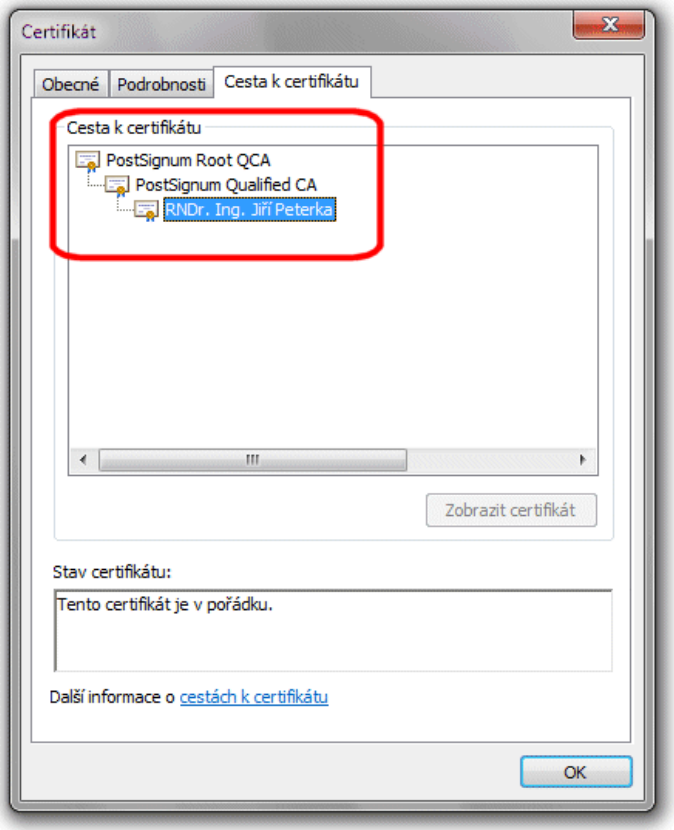
1.12.3 Hierarchie certifikátů a certifikační cesty

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).



Obrázek 1-26: Příklad certifikační cesty konkrétního certifikátu

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: 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, skrze jejich uložení do (správné části) toho úložiště certifikátů, které daný program používá.

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 in-

frastruktury veřejného klíče (PKI). Spolu s tím jsme předpokládali, že certifikáty vydávají certifikační autority, coby důvěryhodné třetí strany, které také ručí za obsah vystaveného certifikátu.

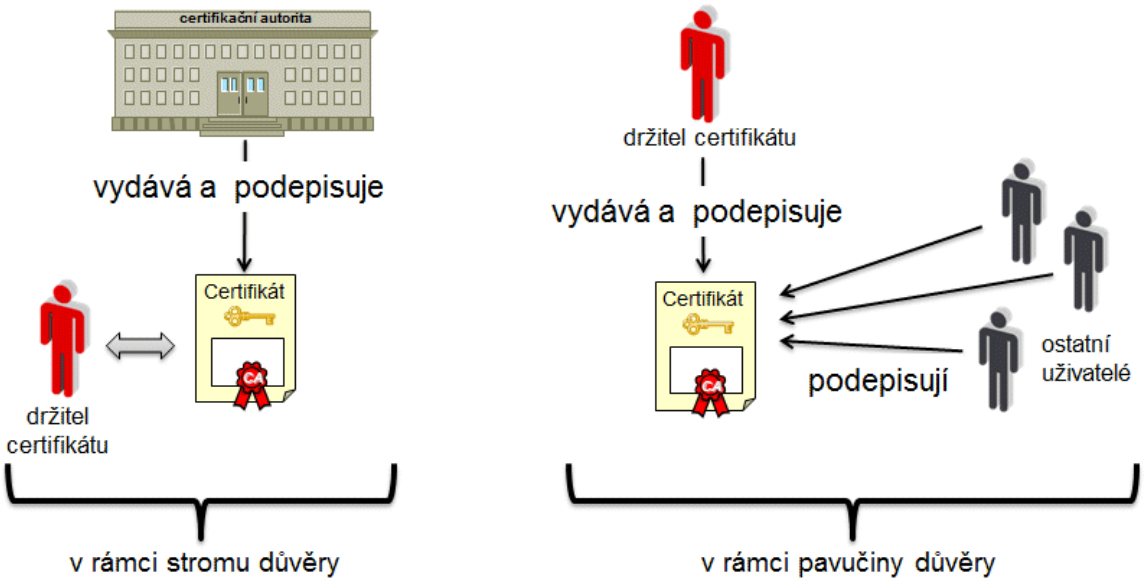
Naši důvěru v konkrétní certifikát a jeho obsah jsme pak odvozovali od důvěry v tuto certifikační autoritu, případně v její nadřazenou certifikační autoritu - protože, jak již víme, certifikační autority mohou v rámci PKI (infrastruktury veřejného klíče) vytvářet hierarchicky uspořádané struktury (stromy),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

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[14]. 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.



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

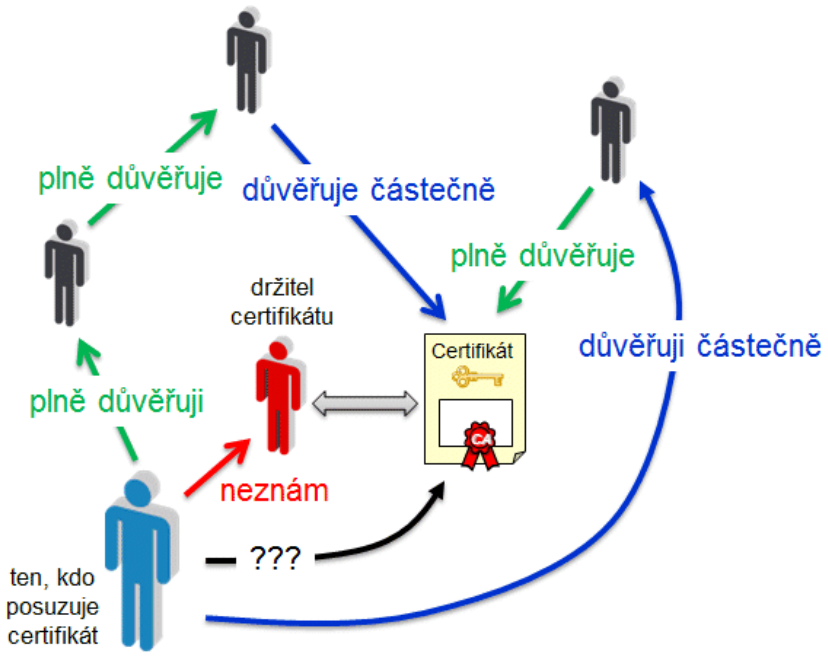
[14] A sami si je také podepisují. Jde tedy o certifikáty tzv. s vlastním podpisem (self signed), jak se dozvíme v dalších kapitolách.

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“.

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%”.

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[15].

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