

# Ověření elektronického podpisu Platanus

*Zkušební dokument*

Verze: **1.0**

Datum: **7.7.2007**

© Matouš Borák, Platanus

### **Upozornění**

Tento dokument je veřejný. Přejete-li si dokument nebo jakoukoli jeho část zkopírovat, upravit či jakkoliv jinak použít mimo osobní účely, nejprve se prosím ujistěte, že k tomu máte výslovný souhlas autora dokumentu.

# Obsah

<b>Historie dokumentu</b> .....	<b>4</b>
<b>Co možná o tomto dokumentu nevíte</b> .....	<b>4</b>
<b>1 Teorie</b> .....	<b>5</b>
1.1 K čemu to je .....	5
1.2 Jak to funguje? .....	5
1.2.1 Důvěra ve třetí stranu .....	5
1.2.2 Vazba certifikátu na podpis .....	6
1.2.3 Otisk dokumentu .....	6
1.2.4 Zneplatnění certifikátu .....	7
1.2.5 Shrnutí .....	7
<b>2 Praxe</b> .....	<b>9</b>
2.1 Oficiální dokumenty Platanus .....	9
2.2 Elektronický podpis dokumentů Platanus .....	9
2.3 Ověření elektronického podpisu .....	9
2.4 První (a neúspěšný) pokus .....	10
2.5 Instalace certifikátů certifikační autority .....	10
2.6 Nastavení Adobe Readeru .....	13
2.7 Druhý pokus a vítězství .....	14

## Historie dokumentu

Verze	Datum	Autor	Popis změn
1.0	7.7.2007	Matouš Borák	Úvodní verze dokumentu

## Co možná o tomto dokumentu nevíte

### Dokument vznikl ve správných rukou

Elektronická verze tohoto dokumentu ve formátu PDF je opatřena tzv. *zaručeným elektronickým podpisem*, který oficiálně garantuje jeho původ. Úspěšné ověření tohoto podpisu Vám zaručuje, že jej vytvořila (resp. alespoň podepsala) osoba uvedená v informacích přiložených k podpisu. K tomu, abyste byli schopni elektronický podpis ověřit, musíte mít náležitým způsobem nastaven program pro prohlížení dokumentů. Přesný postup pro nastavení programu Adobe Reader a ověření podpisu naleznete na webu Platanus, konkrétně na stránce [http://www.platanus.cz/clanky/overeni\\_podpisu](http://www.platanus.cz/clanky/overeni_podpisu).

### Ty podivně velké okraje textu jsou záměrné

... a slouží jako prostor pro Vaše poznámky! A kromě toho tento dokument šetří Vaše oči, neboť má – na rozdíl od většiny jiných podobných dokumentů – sazbu hlavního textu zúženou na typograficky vhodnější velikost. Dokument je navržen pro oboustranný tisk a podporuje tak snižování spotřeby papíru.

### Další informace na webu

Na webu <http://www.platanus.cz> naleznete další informace týkající se nejen projektu, jehož součástí je tento dokument, ale také např. kontaktní informace na autora dokumentu, jeho aktuální časové vytížení, popis poskytovaných služeb, atd.

# 1 Teorie

Dostali jste ode mne oficiální elektronický dokument (fakturu, smlouvu, dokumentaci projektu apod.), otevřeli jste jej a vyskočilo na Vás okénko, které Vám sděluje cosi o neplatném elektronickém podpisu? Nevíte, co s tím – nikdy jste nic takového snad ani neviděli? Tento článek Vám pomůže. Pokud jste ovšem „v obraze“ a jen hledáte přesný postup, přeskočte rovnou níže.

## 1.1 K čemu to je

Obyčejné papírové dokumenty, které ale mají mít určitou váhu, jednoduše opatřujeme naším *vlastnoručním podpisem*. Tím je k dokumentu (většinou) nezpochybnitelně připojena identita toho, kdo dokument podepsal, tj. znamená to: ano, *byl(a) to on(a)*! Můžeme se sice pokoušet podpis napodobit nebo jej různě kopírovat na upravený dokument, důkladná analýza by nás ale měla odhalit.

Ve světě *elektronických dokumentů* je vše složitější. Elektronické soubory jsou jenom shluky jedniček a nul, uspořádaných v nějakém formátu. Pro znalce není až tak těžké takový formát pochopit a *dokument pozměnit* (upravit třeba číslo konta na faktuře)...

A je tu další problém: *odkud ten dokument přišel?* Mohl jsem vám jej doručit osobně na disketě, ale to dnes už dost těžko, mnohem pravděpodobněji vám přišel emailem. Nemohl ten email někdo po cestě zachytit a upravit přílohu? Ale jistěže mohl! Email není žádný zaručený komunikační kanál – vy snad víte, kdo vám posílá spamy?

Shrňme si to: obyčejné elektronické dokumenty v dnešní době *nemůžeme brát moc vážně* – nemáme jistotu, že jej opravdu psal ten, o kom si to myslíme, ani nemůžeme vědět, jestli nebyl někdy během své existence pozměněn.

A právě proto byl vymyšlen koncept elektronického podpisu. Způsobů jeho praktické realizace se vynořilo hodně, tím v současnosti nejrozšířenějším ale je tzv. *elektronický podpis založený na infrastruktuře veřejných klíčů* (tenhle hrozivě složitý název zde nebudu příliš rozebírat a omezím se, stejně jako v celém článku, jen na takové detaily, které umožní základní pochopení věci).

Ať už ta slova znamenají cokoliv, praktickým důsledkem je to, že dokument, který je opatřen takovýmto typem podpisu, a jehož *podpis je při ověření platný*, dává příjemci jistotu v následujících věcech:

- dokument podepsal člověk, jehož personálie jsou uvedeny v informacích připojených k podpisu (v tzv. *osobním certifikátu*),
- od té doby, co byl dokument podepsán, nebyl *žádným způsobem změněn*,
- (trochu méně podstatná vlastnost:) dokument *zaručeně existoval* někdy v době, po kterou je certifikát platný (obvyčně 1 rok).

## 1.2 Jak to funguje?

Poté, co jste si přečetli předchozí odstavec, si teď možná říkáte: no dobrá, dejme tomu, že mám jistotu, že dokument podepsala osoba, která je uvedena v certifikátu připojeném k podpisu, ale *jak mám vědět, kdo to doopravdy je?* – tedy že jde o konkrétní osobu – Matouše Boráka, se kterým jsem dohodnutý na převzetí dokumentu?

### 1.2.1 Důvěra ve třetí stranu

Dostáváme se k hlavnímu principu elektronických podpisů založených na infrastruktuře veřejných klíčů, a tím je *princip důvěry ve třetí stranu* – tzv. *certifikační autoritu*. Podle tohoto

principu při ověřování podpisu nemusíte důvěřovat přímo mně ani nikomu jinému konkrétnímu, ale právě certifikační autoritě.

*Certifikační autorita* je instituce, která lidem vydává osobní certifikáty, jakési *elektronické občanky*, a umožňuje ostatním lidem zjistit jejich platnost, a dělá to všechno vysoce *kompetentním a důvěryhodným způsobem*.

*Osobní certifikát* vydaný autoritou je pak vlastně jen určitý shluk informací o osobě, pro kterou byl vydán, tj. její jméno, adresa, u podnikatelů IČ a další údaje, jako např. doba platnosti certifikátu, apod. Certifikát sám o sobě je chráněn „razítkem“ autority a při jakémkoliv pokusu o „sáhnutí do jeho vnitřností“ okamžitě pozbývá platnosti. Je to ekvivalent běžné „papírové“ občanky, avšak dokonce nejspíš odolnější proti zfalšování.

Opravdu, získat takový oficiální certifikát není jen tak. Žadatel se musí *osobně dostavit na certifikační autoritu*, která si jej důkladně prověří (včetně předložení dvou fyzických dokladů totožnosti), vyplnit několik formulářů a vše několikanásobně stvrdit svým vlastnoručním podpisem. Celá tato „buzerace“ slouží k tomu, aby vydaný certifikát obsahoval opravdu ověřené informace a celý proces byl naprosto neprůstřelný.

## 1.2.2 Vazba certifikátu na podpis

Tak dobrá, zase možná pochybujete, řekněme, že věřím tomu, že k podpisu je připojený certifikát, který jednoznačně patří Matouši Borákovi. Jak ale můžu vědět, že ten certifikát k podpisu někdo nepodstrčil? Řeknu vám to.

Ještě jsme totiž nezmínili jednu kriticky důležitou součást certifikátů používaných v elektronických podpisech – *veřejný klíč*. Je to – co jiného – zase nějaký shluk bajtů, ale to nás v tuto chvíli nemusí vůbec zajímat, podstatné je, že veřejný klíč (jako každý kryptografický klíč) slouží ke kódování zpráv a především, že je *jednoznačně* a „nerozlučně“ spárován s tzv. *privátním klíčem*.

Co to znamená? Chytré matematické hlavy vymyslely speciální kódovací funkce, které pracují na principu ne jednoho, ale *dvojice klíčů*. Funguje to následovně: vezmu zprávu a zakóduji ji svým *privátním klíčem*. Výsledek předám příjemci, ten si někde sežene můj *veřejný klíč* a pomocí něj zprávu zase rozkóduje. A figl je v tom, že se mu to nepovede ničím jiným než právě oním druhým klíčem z páru, veřejným klíčem.

Jenže *jak to souvisí s elektronickým podpisem*? Mám pocit, že už se to trochu rýsuje: chci-li podepsat nějaký dokument, vezmu svůj privátní klíč a pomocí něj dokument zakóduji do nějaké datové zprávy. Tu přibalím k dokumentu a vše pošlu příjemci. Ten si vyhledá můj veřejný klíč, s jeho pomocí datovou zprávu rozkóduje a pokud výsledek odpovídá samotnému dokumentu, má *jistotu, že tento dokument byl zakódován (tj. podepsán) právě mnou*, neboť použitý veřejný klíč je jednoznačně spojen s mým osobním certifikátem.

## 1.2.3 Otisk dokumentu

Ale jelikož kódování je výpočetně náročná činnost a protože výše uvedený postup způsobí, že se dokument vlastně přenáší dvakrát (v otevřené formě a zakódovaný), ve skutečnosti se nepodepisuje celý dokument. Místo toho se z něj nejprve vypočítá nějaká malá datová zpráva, která se k dokumentu jednoznačně váže (tj. říká *ano, toto je právě ten a ten dokument!*). Říká se jí *otisk dokumentu* neboli „hash“. A vazba je to opravdu ultimativní – stačí změnit jedině písmenko v dokumentu a jeho otisk se rázem úplně změní.

Výše uvedený základní postup při elektronickém podepisování tedy prakticky probíhá následovně:

- odesílatel nejprve:
  - » vypočte otisk dokumentu,

- » tento otisk pak zakóduje svým privátním klíčem a výsledek přiloží k dokumentu jako jeho elektronický podpis,
- » k obojímu ještě přibalí svůj osobní certifikát, ve kterém je uložen mj. také jeho veřejný klíč
- » to vše zašle příjemci
- příjemce pak:
  - » vypočte otisk přijatého dokumentu,
  - » vezme z přiloženého certifikátu veřejný klíč odesílatele a s pomocí něj rozkóduje otisk, který je součástí podpisu,
  - » porovná svůj vypočtený otisk s tím z podpisu a pokud jsou shodné, má jistotu, že podepsaný dokument je právě ten, který má před sebou,
  - » pak se podívá, čím je to vlastně veřejný klíč, kterým rozluštil podpis – tj. podívá se do přibaleného certifikátu,
  - » aha, tady se píše, že je to „ten a ten“ odesílatel – můžu tomu věřit? a podívá se, kdo vydal tento certifikát
  - » v případě, že byl certifikát vydán autoritou, které příjemce důvěřuje, má jistotu také v tom, že dokument podepsal opravdu ten člověk, který je v certifikátu uvedený

Uf! Vypadá to příšerně složitě, že? Útěchou nechť vám je fakt, že všechny tyto složitosti za vás při ověřování podpisu *počítač udělá sám* a vy to všechno můžete s klidem zase zapomenout...

#### 1.2.4 Zneplatnění certifikátu

Ještě než tak učiníte nám tu ale zbývá ještě jedna věc. Pořád dokola jsme mluvili o privátním klíči a veřejném klíči. Ty názvy něco evokují. Ano, je to tak, zatímco veřejný klíč je opravdu veřejná informace, kterou si může kdokoliv vyhledat, *privátní klíč je věc nesmírně citlivá*. Vždyť kdyby se někdo dostal k mému privátnímu klíči, mohl by mým jménem podepisovat dokumenty a nikdo by nepoznal, že to nebylo mou „rukou“! Tady by nepomohla žádná grafologická analýza, bity a bajty jsou prostě stejné, ať jsou vytvořeny kýmkoliv.

Privátní klíč si tedy musí každý vlastník hlídat jako oko v hlavě. Svět ale není dokonalý, co když se přece jen stane, že se k mému klíči dostane někdo, kdo nemá? Například zloděj, který mi ukradl notebook, nebo pokud klíč prostě ztratím a někdo jej najde? Pro tyto případy poskytují certifikační autority záchrannou službu zvanou *zneplatnění neboli revokace certifikátu*.

Jakmile já, jako vlastník privátního klíče a příslušného certifikátu, zjistím, že už svůj privátní klíč nemám pod svou výhradní kontrolou, okamžitě bych měl informovat certifikační autoritu, která certifikát vydala, a *nechat certifikát zneplatnit*. Je to podobné situaci, kdy zoufalí voláte do banky a necháte zablokovat svou ukradenou kreditní kartu. Autorita pak informaci o zneplatnění certifikátu přidá do *seznamu zneplatněných certifikátů*, který je veřejně dostupný na internetu.

Co z toho vyplývá pro ověřování elektronického podpisu? Vyplývá z toho poslední povinnost při ověřování podpisu a tou je právě *kontrola seznamu zneplatněných certifikátů*. Příjemce by měl vždy při ověřování podpisu zkontrolovat tento seznam, aby měl jistotu, že certifikát podpisu nebyl mezitím zneplatněný a že je tedy vše v pořádku. Když to neudělá, pak přestože je jinak podpis třeba platný, chybí tu ta absolutní jistota, že ve skutečnosti nebyl podpis někým zneužit. Je zřejmé, že v praxi je k tomuto kroku kontroly nutné být připojen k internetu.

### 1.2.5 Shrnutí

Pokud jste zvládli dočíst až sem, vězte, že jste právě vstřebali kompletní základy rozsáhlé problematiky elektronických podpisů založených na infrastruktuře veřejných klíčů. Gratuluji!

Co tedy musíte (resp. váš počítač musí) udělat pro ověření elektronicky podepsaného dokumentu:

- musíte ověřit otisk dokumentu, čímž se ujistíte, že **nebyl po podepsání pozměněn**,
- musíte ověřit, že přiložený certifikát by vydán certifikační autoritou, které důvěřujete; pokud ano, pak máte jistotu, že člověk uvedený v certifikátu je ten, kterého očekáváte, a že **právě on dokument podepsal**,
- a konečně musíte ověřit, že se certifikát nenachází na seznamu zneplatněných certifikátů, čímž **získáte jistotu, že podpis nebyl někým zneužit**.

Nyní byste již měli tušit, co se děje, když na vás vyskočí ono v úvodu zmiňované okénko. V každém případě můžete směle přikročit k ověření elektronického podpisu v praxi.

## 2 Praxe

### 2.1 Oficiální dokumenty Platanus

Veškeré oficiální dokumenty, které ode mne obdržíte elektronickou cestou (mohou to být faktury, smlouvy, dokumentace k projektu, apod.), jsou podepsány mým elektronickým podpisem. Dokumenty jsou šířeny ve formátu PDF.

*Proč právě formát PDF? Má několik bezvadných výhod:*

- je všeobecně velmi známý a rozšířený
- existuje pro něj prohlížeč Adobe Reader, který si můžete [stáhnout zdarma](#) (ale jistě už jej máte)
- a co nás nyní zajímá nejvíce, *má velmi propracovanou podporu elektronických podpisů*:
  - » podpis je uchovávan přímo v dokumentu (nemusí se k němu nějak složitě přikládat)
  - » ověření podpisu je při správném nastavení programu naprosto automatické a pro uživatele intuitivní, jak za chvíli sami uvidíte!

Tento článek předloží postup pro ověření podpisů v dokumentech PDF s využitím nejnovějšího prohlížeče *Adobe Reader verze 8* (update 8.1) na Windows.

### 2.2 Elektronický podpis dokumentů Platanus

K podepisování dokumentů používám tzv. *kvalifikovaný certifikát*. Ten se od běžných certifikátů liší především tím, že jeho získání a používání se přesně řídí speciálním zákonem, konkrétně [Zákonem 227/2000 Sb. o elektronickém podpisu](#), což certifikátu dodává oficiální punc.

Certifikát je navíc vydaný tzv. *akreditovanou certifikační autoritou*, jejíž provoz opět musí být v přesném souladu se zákonem. Co z toho všeho vyplývá? Soulad se zákonem staví takový elektronický podpis v elektronické komunikaci *na roveň podpisu vlastnoručnímu*. A to dokonce tak, že jej uznávají i české úřady...! Jednoduše je to stejné, jako kdybych vytištěný dokument podepsal vlastní rukou.

V Česku jsou v současné době v provozu tři akreditované certifikační autority, v mém případě je to instituce přidružená k *České poště*, zvaná [PostSignum](#). Právě ta mi vydala certifikát, kterým podepisuji dokumenty.

### 2.3 Ověření elektronického podpisu

Nyní budu předpokládat, že máte k dispozici dokument, který je mnou pravděpodobně podepsaný, a chcete jej náležitě ověřit. Jinými slovy tedy chcete provést následující kroky:

**zkontrolovat otisk dokumentu**, abyste se ujistili, že dokument nebyl po podepsání pozměněn,

**zkontrolovat údaje v certifikátu** připojeném k podpisu, zda se týkají mé osoby,

ujistit se, že certifikát byl **vydaný autoritou, které důvěřujete**, a že tedy můžete důvěřovat i tomuto certifikátu

a konečně potřebujete **zkontrolovat seznam zneplatněných certifikátů** vydaných touto autoritou, abyste měli úplnou jistotu, že certifikát (a s ním i podpis) nebyl od jeho vydání zneužit.

Vypadá to možná složitě, mohu vás ale ujistit, že většinu kroků za vás udělá počítač a vy, jako člověk, budete muset provést vždy jen krok číslo 2 – prohlédnout informace

v certifikátu – a i ty vám prohlížeč dokumentu donese až přímo „pod nos“. K tomu, jak jej nastavit, aby to opravdu dělal, se konečně dostáváme nyní. Takže, jde se klikat!

## 2.4 První (a neúspěšný) pokus

Nejprve zkusme dokument otevřít tak jak je, bez nějakého nastavování čehokoliv. Otevřete PDF dokument a v Adobe Readeru 8 uvidíte něco podobného, jako na obrázku na následujícím straně nahoře (u dřívějších verzí Readeru se bude zobrazení informací o podpisu lišit, princip však zůstává stejný):

Čeho si na obrázku všimnout? Především, nahoře je modrá lišta, která zobrazuje informace o právě ověřovaném podpisu dokumentu. Na liště je bezútěšná hláška o tom, že dokument je sice podepsán, ale *identita podepisující osoby je neznámá* – lidsky řečeno: *tomuto podpisu nevěříme!* Tedy aspoň prozatím...

Dole na stránce, pod datem vydání dokumentu, je umístěn *samotný elektronický podpis*. PDF dokumenty umožňují k podpisu přiřadit nějaký obrázek, v tomto případě jde drze o můj opravdový „ruční“ podpis, který jsem předtím naskenoval. U podpisu je zobrazena ikonka s panáčkem a otazníkem, která intuitivně vybízí k zostření pozornosti – něco s podpisem není v pořádku.

Na pravé straně lišty je tlačítko, které zobrazí *podrobnosti o podpisu dokumentu* (viz obrázek dole).

Tam je souhrnným způsobem uvedeno, kdo podpis provedl, z jakého důvodu a kdy a kde. Pod tím se nachází shrnutí celého procesu ověření podpisu. Je tam postupně uvedeno, že:

- (zelená fajfka) dokument nebyl pozměněn od doby podpisu, jinými slovy, což je fajn,
- (otazníček) certifikát podepisující osoby byl vydán autoritou, které doposud nedůvěřujete – *aha to je ten problém!*
- a (výstražný trojúhelník) konečně, že čas podpisu je založen na času v mém počítači a nemusí být na 100% důvěryhodný, což je nám teď ale celkem jedno.

## 2.5 Instalace certifikátů certifikační autority

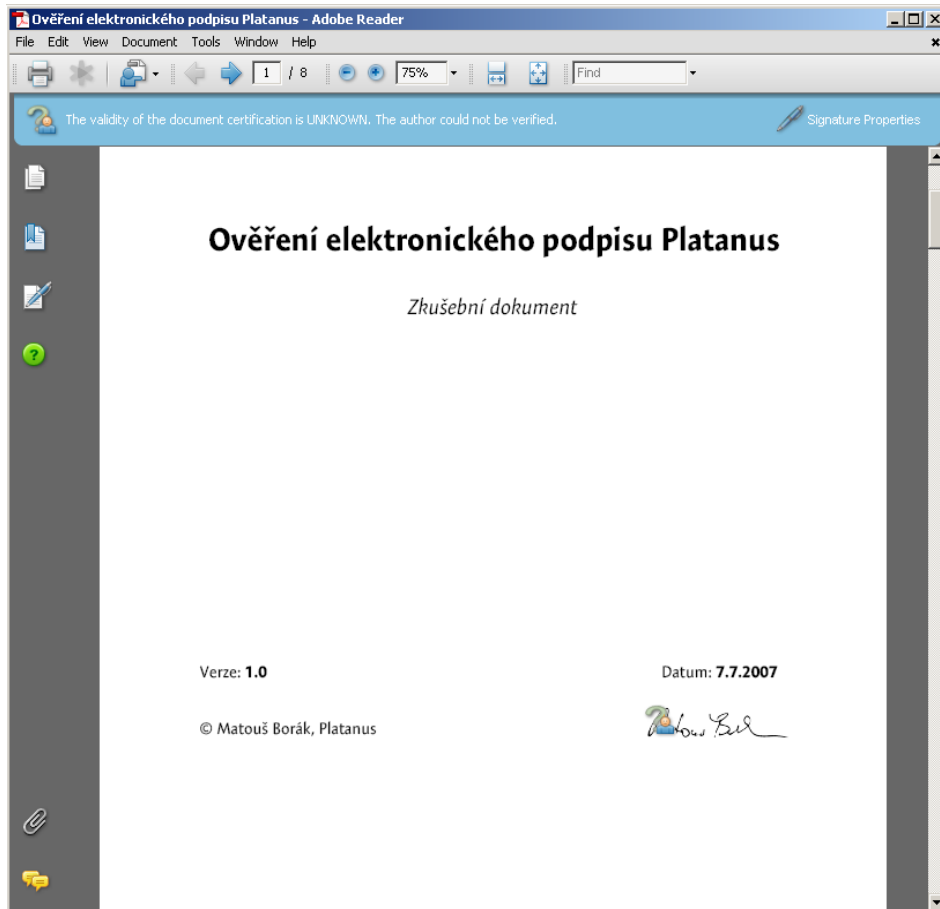
Předchozím pokusem jsme zjistili, že prohlížeč podpis nepovažuje za platný, neboť nedůvěřujeme certifikační autoritě, která vydala podpisový certifikát. *Jak ale zařídit důvěru v tuto autoritu?*

Využitím certifikátů certifikační autority. Ano, i autority mají své certifikáty, které slouží jako jejich občanské průkazy, kterým rozumějí počítače. Kde je vzít? Nejlépe z nějakého důvěryhodného zdroje, například z oficiálního webu autority. *Certifikáty autority PostSignum* jsou k mání na adrese <http://qca.postsignum.cz/www/authorities.php>.

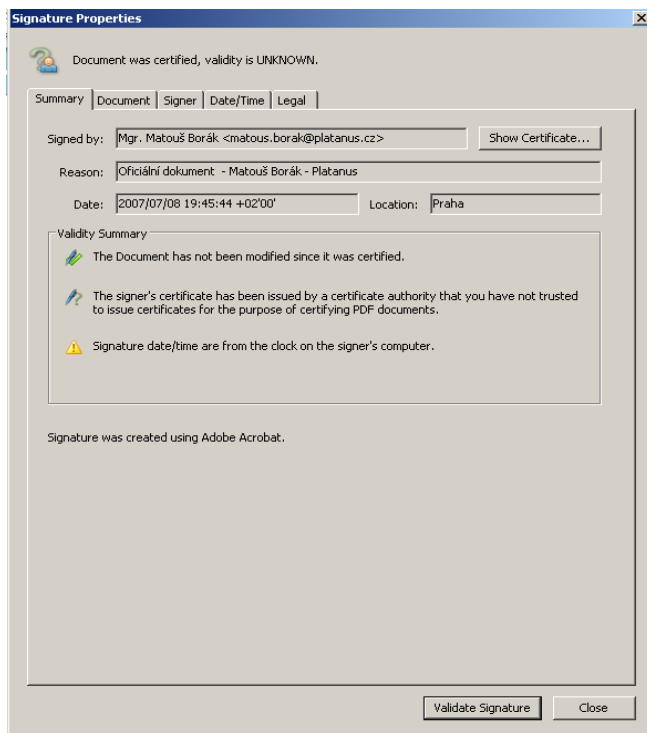
Nyní musím udělat drobnou, ale nutnou technickou odbočku. Certifikační autoritu PostSignum ve skutečnosti reprezentují dva certifikáty, které jsou v hierarchickém vztahu. První je certifikát tzv. kořenové autority, druhý patří podřízené autoritě. Proč to tak je, nás nyní vůbec nemusí pálit, podstatné je, že pro ověřování podpisů *potřebujeme oba dva*.

Stáhněte si tedy oba certifikáty (kořenové i podřízené autority) k sobě na počítač. Stahujte certifikáty ve formátu DER (tj. ty soubory, které mají příponu **.cer**), neboť Windows si rozumí právě s tímto formátem. Co teď s nimi? Windows obsahují takzvaná *úložiště důvěryhodných certifikátů*. Přidáte-li nějaký certifikát do takového úložiště, automaticky se pro systém, potažmo i pro vás, stává důvěryhodným. Je to takový šuplík s cedulkou *Věcem uvnitř důvěřuji*.

U certifikátů certifikační autority jsou dopady jejich přidání do úložiště Windows ještě silnější – říkáte tím, že *důvěřujete této autoritě jako celku a tedy i všem certifikátům, které*



Okno Adobe Readeru při neúspěšném pokusu o ověření podpisu



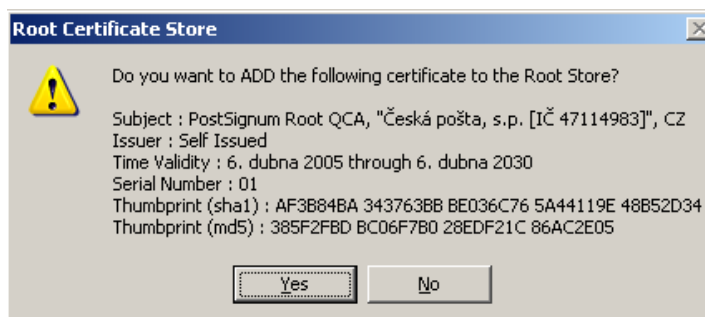
Detaily nedůvěryhodného elektronického podpisu

sama vydala. Tím se naplňuje princip důvěry ve třetí stranu, zmiňovaný v teoretické části článku.



Certifikát se do úložiště přidá jeho *nainstalováním*. To se provede prostým otevřením certifikátu (dvojitým kliknutím na něj). Začneme kořenovým certifikátem, tj. souborem `postsignum_qca_root.cer`. Objeví se okno podobné tomu na obrázku vlevo:

Červený křížek jasně naznačuje, že tomuto certifikátu prozatím nevěříme. Zvolte tlačítko „Nainstalovat certifikát...“ a projděte celým průvodcem beze změn přednastavených hodnot, až se dostanete k okýnku, které je uvedeno na obrázku dole. Je to poslední výzva předtím než se certifikát autority přidá do úložiště důvěryhodných certifikátů. Měli byste si nyní uvědomit, že odsouhlasení této výzvy je *velice delikátní záležitost*. Jde do tuhého...



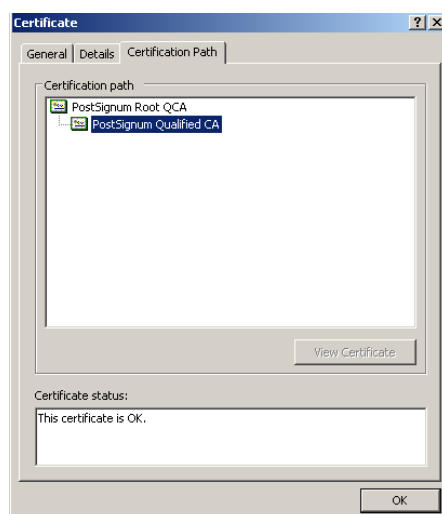
Tím, že nyní kliknete na „Ano“, vlastně sdělujete svému počítači následující: *Ano, důvěřuji této certifikační autoritě. Důvěřuji také všem platným certifikátům, které byly touto autoritou vydány. A tím pádem také budu považovat za důvěryhodné všechny elektronické podpisy, které byly vytvořeny s použitím těchto certifikátů.*

Začínáte se mírně potit? Rosí se vám čelo? To je dobře, protože s důvěrou v certifikační autority si není radno bezmyšlenkovitě zahrávat. Paranoici mohou, pro úplnou jistotu, že přidávají ten správný certifikát, *zkontrolovat jeho otisk*, který je uveden na výzvě na obrázku vpravo, s oficiálním otiskem, který získal od nějakého důvěryhodného zdroje (je uveden také na stránkách PostSignum). Ale řekněme, že svět není tak zlý a odsouhlasme výzvu.

Tím jsme přidali kořenový certifikát autority do úložiště důvěryhodných certifikátů. Pokud nyní dialog zavřete a znovu na certifikát poklepáte, už byste neměli vidět červený křížek – *váš systém nyní tomuto certifikátu věří.*

Provedte nyní podobnou instalaci i s *druhým certifikátem* – souborem `postsignum_qca_sub.cer`. Nelekejte se, že vám systém nyní nepředloží žádnou výzvu na konci průvodce instalací. U tohoto typu certifikátu (podřízené autority) je to správně.

Po dokončení instalace můžete přejít na záložku „Cesta k certifikátu“ a měli byste vidět oba nové certifikáty hezky pod sebou, hierarchicky uspořádané a bez červených křížků, vykřičníků či jiných varování, podobně jako na obrázku:

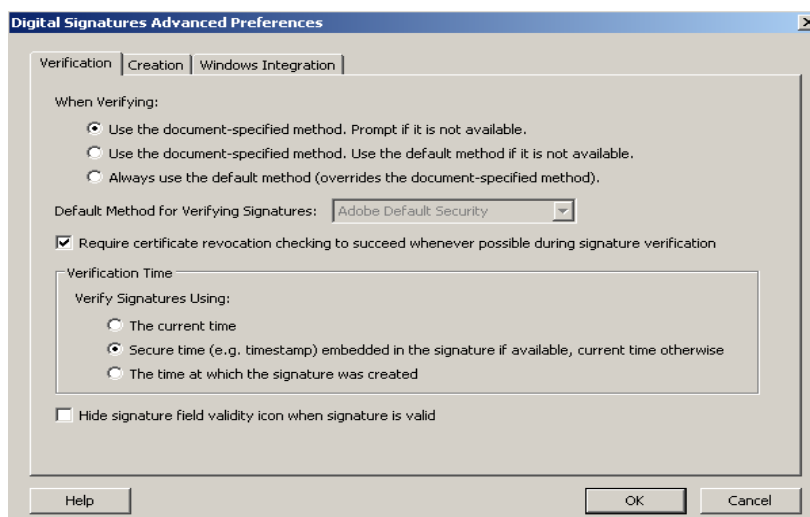


Tak, tímto jste začali důvěřovat mému osobnímu certifikátu. Zbývá nastavit samotný prohlížeč dokumentů.

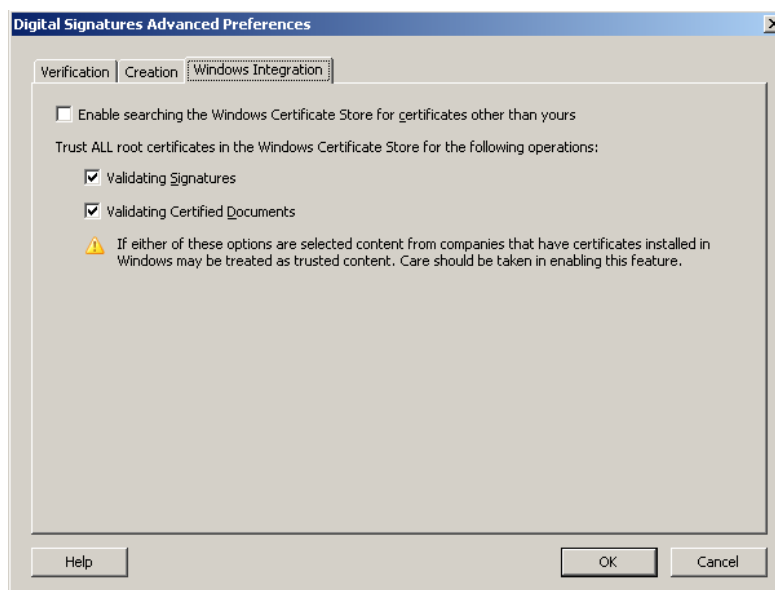
## 2.6 Nastavení Adobe Readeru

První krok výše zmíněného postupu – ověření otisku dokumentu – za vás udělá Adobe Reader automaticky a není třeba nic nastavovat. Dvojku musíte zvládnout sami, ale už jste si to jednou vyzkoušeli a víte, že k tomu slouží horní lišta Readeru. Třetí krok, tj. důvěru v certifikační autoritu, jsme si právě zařídili, ovšem jen na úrovni operačního systému. Zbývá o tom informovat ještě Adobe Reader a také nastavit poslední, čtvrtý krok – kontrolu seznamu zneplatněných certifikátů.

Otevřete Adobe Reader a přejděte do „Nastavení programu“ (v menu „Úpravy“). Tam v levém sloupci vyberte položku „Zabezpečení“ a klikněte na tlačítko „Pokročilé nastavení“. Měli byste vidět něco podobného jako na obrázku:



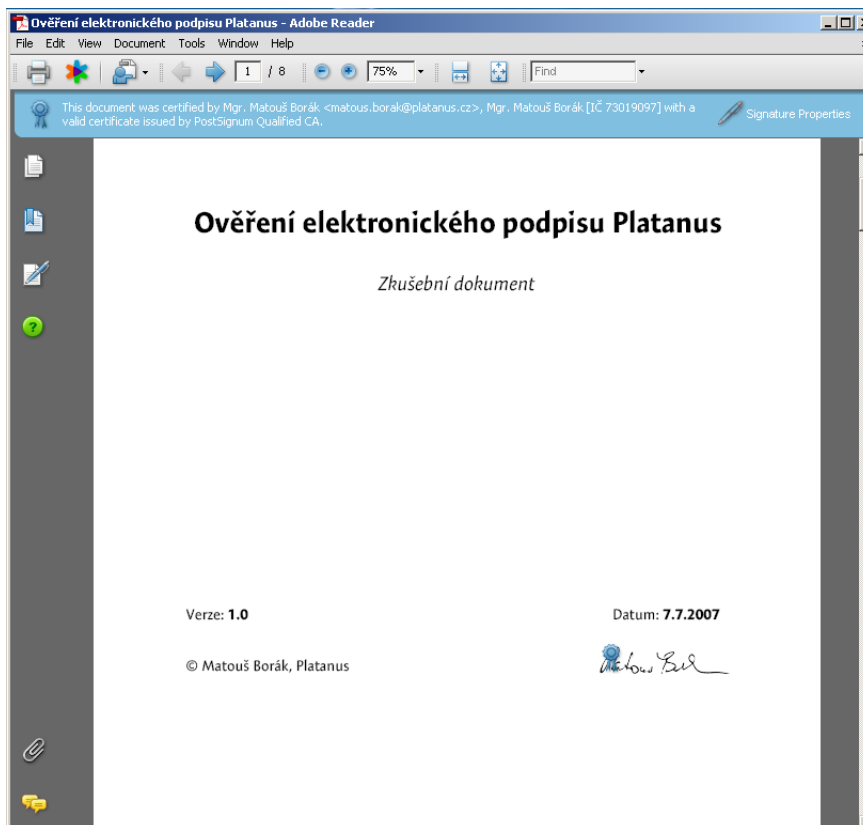
Fajn, ponechte ale teď toto okno osudu a přejděte rovnou na třetí záložku s názvem „Integrace s Windows“ (viz obrázek dole). Tam zaškrtněte obě políčka, podobně jako na obrázku. Právě tím říkáte Adobe Readeru, *aby při ověřování certifikátů bral v potaz centrální úložiště důvěryhodných certifikátů Windows*, kam jsme před chvílí přidali certifikáty autority.



Zbývá poslední úkol – *kontrola seznamu zneplatněných certifikátů*. Přejděte zpět na první záložku (předchozí obrázek) a ujistěte se, že je zaškrtnuto políčko zhruba uprostřed stránky, které říká něco jako „Vyžadovat, aby kontrola zneplatnění certifikátů při ověřování podpisů dopadla úspěšně vždy, když je to možné“.

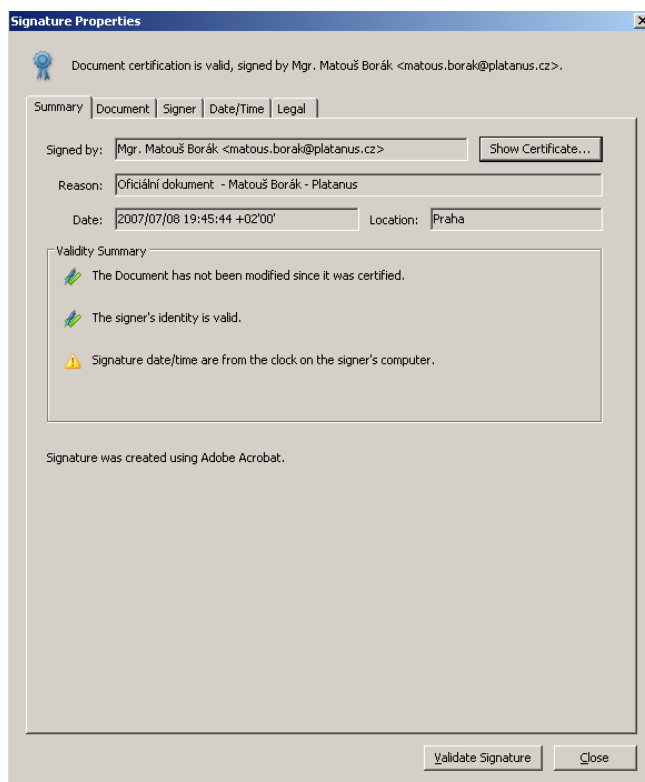
Tím říkáte Readeru, aby se vždy snažil zkontrolovat seznam zneplatněných certifikátů při ověřování podpisu. Jak víme z teoretické části, *seznam zneplatněných certifikátů je dostupný na internetu* a stará se o něj certifikační autorita. Proto, pokud náhodou k internetu nejste běžně připojeni, tuto volbu spíše odškrtněte a kontroly zneplatnění certifikátu se pak musíte vzdát.

Potvrďte provedené změny a jásejte, neboť jsme u konce s nastavováním!

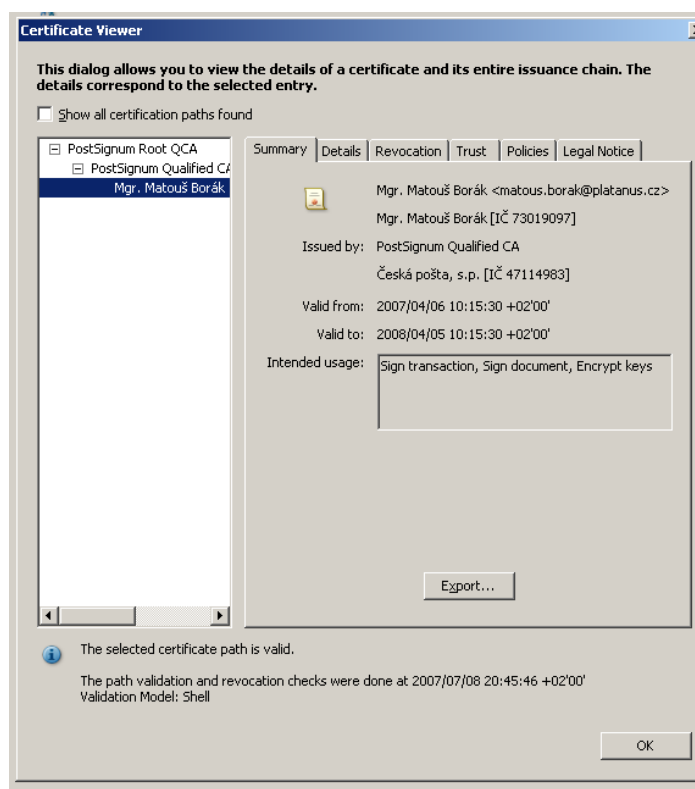


Okno Adobe Readeru při úspěšném ověření elektronického podpisu

## 2.7 Druhý pokus a vítězství



Detaily úspěšně ověřeného elektronického podpisu



*Detaily certifikátu připojeného k elektronickému podpisu*

Otevřete nyní podruhé podepsaný dokument a tentokrát byste měli vidět něco podobného jako na obrázku na následující straně nahoře. Něco se změnilo, vidíte? Předně si horní lišta již nestěžuje na neznámou identitu ale naopak *uvádí mé jméno coby podepisující osoby* a další údaje, které mě pomohou jednoznačně identifikovat. Dole na stránce už u mého podpisu „nestraší“ otazník, ale je tam pěkná modrá pečeť symbolizující, že je vše v pořádku.

Detaily podpisu (obrázek dole) jsou téměř stejné jako předtím, s jednou podstatnou změnou – uprostřed shrnutí je konečně „černé na šedém“ napsáno, že *identita podepisující osoby je platná*.

Nakonec uvádím ještě detaily certifikátu dostupné pomocí tlačítka „Zobrazit certifikát“ vpravo (viz poslední obrázek dokumentu). V detailech je v levém sloupci krásně vidět celá hierarchie certifikátů, od kořenového certifikátu autority až po můj osobní certifikát. Dole pak je zobrazena informace o provedené kontrole seznamu zneplatněných certifikátů.

*A to je vše! Takže, bylo to jednoduché nebo ne? Přeji hodně nezklamané důvěry jak při ověřování podpisů v dokumentech Platanus, tak i obecně při spolupráci se mnou!*