Důvěřuj, ale prověřuj

Víte vůbec, kdo je na druhém konci?

PATRIK MALINA

Bez nadsázky lze říci, že jednou z nejvýznačnějších vlastností mnoha internetových služeb, způsobujících jejich příslovečný lesk i bídu, je anonymita. Při používání velmi populárních komunikačních nástrojů pro chatování se skrýváme za přezdívkami, webové stránky navštěvujeme zásadně anonymně, e-maily si posíláme pomocí veřejných služeb opět pod falešnými jmény, a o často ne zcela legálních aktivitách prostřednictvím výměnných sítí netřeba déle mluvit.

Ba co více, i v případě, kdy se obě strany komunikace přiznávají ke svým jménům, což je případ obzvláště e-mailové komunikace, nikdy nemáte jistotu, že vás protějšek nechce zmást a svou identitu pouze nepředstírá.

Uvedený fakt je pochopitelně zásadním kamenem úrazu při snaze o nasazení internetu v důvěryhodné komunikaci, jež je nezbytná při uzavírání obchodních transakcí či jiných „seriózních" aktivitách. Právě aplikace jako internetové bankovnictví či nákupy po internetu si vyžádaly zavedení spolehlivého mechanismu, jak si obě strany komunikace vymění důvěryhodnou informaci o své identitě bez toho, aby se osobně setkaly. Jen si vzpomeňte na své internetové zkušenosti: kolikrát jste něco nakupovali a potvrzovali platbu přes webové rozhraní? A byli jste si jisti, že třeba číslo kreditní karty odesíláte důvěryhodnému protějšku? Že jste o tom nepřemýšleli? A co když už teď má vaše důvěrné informace někdo, kdo by neměl?

V následujících odstavcích se spolu podrobně podíváme na to, jak jsou otázky ověření totožnosti a potvrzení důvěryhodnosti při každodenní internetové komunikaci řešeny. Ukážeme si, že běžně využívané aplikace nabízejí dostatek možností pro dostatečnou míru zabezpečení, a řekneme si o zásadách, jejichž dodržování by mělo být samozřejmostí. Koneckonců, nejde o nic menšího než o naše soukromí a peníze, že?

Protože problematika, o níž budeme hovořit, je poměrně rozsáhlá, rozhodli jsme se článek rozdělit na dvě části. V dnešním čísle najdete úvodní část a první konkrétní aplikace, v čísle příštím pak dokončení s řadou dalších ukázek z praxe. A ještě na jednu skutečnost bychom rádi upozornili: předkládaný text si neklade nároky na vyčerpání této nesmírně rozsáhlé tematiky, ani na extrémní přesnost ve formulacích. Kriteriem je pochopení principů a možnost praktického využití, takže prosíme specialisty a znalce o shovívavý přístup.

Jak to všechno pracuje?

Internetová bezpečnost není textový editor. Nelze jen přisednout a vše rázem účelně a dobře využívat, a proto jsme do první části článku zařadili vysvětlení základních principů, bez nichž by věc byla neúplná a jakékoliv popisy samoúčelné a nesrozumitelné. Za svou snahu toto pročíst a pochopit, budete odměněni tím nejcennějším: budete schopni si důsledně ověřit důvěryhodnost, protože celé věci porozumíte.

Není šifra jako šifra, aneb co musíte vědět

Máme-li úspěšně proplout tajemstvím elektronické identifikace a přitom získat plnou důvěru v systém, o němž budeme mluvit, je potřeba lehce nahlédnout do světa šifrování. Nebojte se, žádné vzorce, žádné výpočty, jen úvodní nezbytné vysvětlení. Po řadu tisíciletí, tedy prokazatelně od starých Egypťanů přes Caesara až po Matyase Sandorfa z oblíbeného Verneova příběhu byla šifrovaná komunikace závislá na principu tzv. symetrické šifry: jediný klíč, byť velmi komplikovaný či dlouhý, sloužil k převodu původní zprávy na šifrovanou formu a následně také pro převod opačný, tedy zpět do čitelné podoby. Jinými slovy, když si dvě strany chtěly šifrovaně dopisovat, musely si předem bezpečným kanálem vyměnit klíč pro oboustrannou operaci. Aby jeden partner zprávu zašifroval a druhý přečetl, museli oba dva znát společné, sdílené tajemství (mřížku s otvory, postup čtení, zástupné symboly, číselný kód…). Jistě zde cítíte onu zásadní slabinu, jež spočívala ve způsobu předávání onoho tajného klíče. Jak to učinit v praxi: poštovní obálku může někdo prohlédnout, telefon odposlechnout, živého kurýra unést či podplatit. Jako jedno z mála poměrně spolehlivých řešení se nám jeví osobní setkání obou protistran, což však má podstatnou chybičku – v internetovém světě je to při hustotě naší komunikace naprosto nereálné.

Již v době, kdy byl internet na rýsovacích prknech, si několik lidí tento fakt uvědomovalo a usilovně pracovali na řešení této neodbytné otázky, jež předznamenávala budoucnost: jak si bezpečně a zároveň všem na očích předat šifrovací klíče, aniž by tajemství utrpělo? Zhruba na přelomu 60. a 70. let se objevila první použitelná realizace konceptu, jemuž dodnes běžně říkáme asymetrická kryptografie či kryptografie s veřejným klíčem. Krása tohoto ne zrovna jednoduchého, ovšem geniálního matematického postupu spočívá v tom, že každý účastník komunikace nemá klíč jediný, ale hned klíče dva! Tyto dva klíče vznikají spolu a jsou to nerozlučná dvojčata, neboť jeden bez druhého mnoho nezmůže, avšak zásadně se liší nároky na jejich zabezpečení: jeden z nich, označovaný jako klíč privátní (soukromý), je výhradním tajemstvím majitele a nikdo cizí jej nesmí znát, tedy ani protějšek při komunikaci, který jej navíc nebude vůbec k ničemu potřebovat! Protistrana při komunikaci totiž využívá zásadně a výhradně tzv. klíč veřejný (public key), jenž díky svému sbratření s prvním poskytne potřebnou funkci. Veřejný klíč je doslovným naplněním svého názvu, neboť jeho majitel jej vystavuje na obdiv a říká, že jakoukoliv tajnou informaci může pro něj kdokoliv zašifrovat právě pomocí tohoto veřejného klíče. Základní vlastnost asymetrické šifry je totiž ta, že informaci šifrovanou veřejným klíčem příjemce je posléze možno dešifrovat výhradně a pouze klíčem soukromým – sourozencem, a ten je v tajném držení příjemce. Cítíte tu ohromnou změnu? Když zprávu utajuji, používám zcela veřejnou věc, kterou si mohu klidně stáhnout z internetu, neboť její znalost nestačí ke zpětnému rozlousknutí vzniklého tajemství. Právě tato krásná vlastnost dovoluje věci, o nichž budeme dále mluvit.

Mám certifikát, tedy jsem

Po pročtení našeho letmého úvodu pod nadpisem a malém zamyšlení jasně docházíme k závěru, že dalším krokem na cestě k důvěryhodné komunikaci jakéhokoliv druhu je vybavení všech zúčastněných stran jakýmsi identifikátorem. Bezpečná šifra je sice pěkná věc, ale když nevím, kdo je na druhém konci, nic nezmůže: ochráněný přenos ještě důvěru v komunikační protistranu nevybuduje. Nároky na „internetový identifikační průkaz" nejsou zrovna malé: chceme z něj mimo veškerou pochybnost zjistit, kdo je jeho držitelem, dále jej hodláme používat v různých aplikacích, jež mu musejí pokud možno bez potíží rozumět, a v neposlední řadě musí být uzpůsoben ke snadnému a bezpečnému zasílání po síti. Tedy jakási všestranná, pro všechny zúčastněné čitelná jedinečná vizitka.

Vytvořit žádoucí strukturu nebylo vůbec snadné, avšak dnešní počítačová realita nám nabízí až překvapivě dobré řešení v podobě elektronického dokladu, jemuž říkáme certifikát. V zásadě si tuto „věc", jež slouží jako elektronická občanka, představte jako jiný běžný soubor – lze jej ukládat na disk či přenosné médium (disketa, čipová karta atd.), exportovat či importovat do operačních systémů, a jako soubor také prohlížet či interpretovat. Jednou z hlavních vlastností certifikátu je jeho přesně definovaná struktura: zahrnuje řadu závazných položek, jejichž účelem je především identifikovat jeho držitele, a to mimo veškerou pochybnost a doslova v celosvětovém měřítku. Právě proto jsou obsažená pole nápadně podobná jiným identifikačním průkazům a najdeme zde položky jako sériové číslo, jméno, adresa či období platnosti. Již z tohoto stručného nástinu je patrné, že důkladným porovnáním různých rozpoznávacích polí je možno vyloučit záměny či jednoznačně označit držitele, což je naším cílem. Mezi naprosto klíčová pole certifikátu též náleží údaj, jehož význam jsme nastínili výše. Hádáte správně, je to veřejný klíč pro asymetrickou kryptografii a jeho využití v certifikátu je víceúčelové, jak si ukážeme dále. Tedy, veřejný klíč dostává v podobě certifikátu jasné znaky svého držitele a je pevně přiřazen.

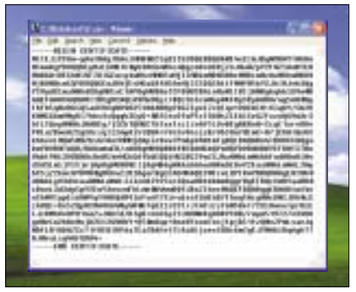
Na tomto místě je potřeba upozornit na jednu důležitou skutečnost, jež možná v předchozích řádcích zcela jasně nezazněla. Ve světě elektronické komunikace nemusí být protějškem vždy uživatel, ale též třeba počítač, někdy si navíc povídají počítače mezi sebou a rovněž si potřebují důvěřovat. Samozřejmě i tyto protistrany potřebují svůj certifikát a pochopitelně jsou jim běžně vydávány, jako je tomu kupříkladu u internetových webových serverů, k čemuž se ještě dostaneme. Zní to podivně? Ale nebuďte přeci tak sebestřední…

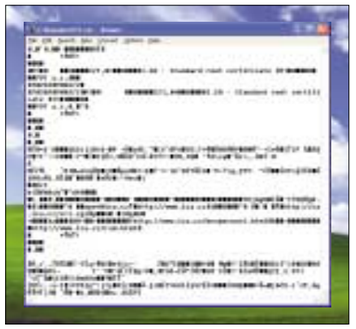
Podoba dnes prakticky používaných certifikátů je přesně specifikována především pomocí dvou základních norem. Jednou z nich je internetový dokument RFC–3280 a druhou pak doporučení ITU X.509. Velmi podrobné informace najdete ve skvělé knize Libora Dostálka Velký průvodce protokoly TCP/IP: bezpečnost (již 2. vydání).

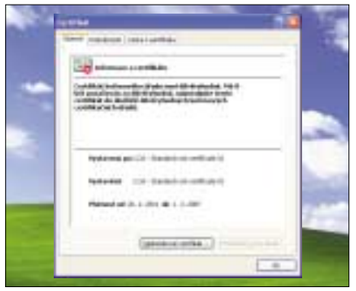
- *http://www.ietf.org/html.charters/pkix-charter.html*

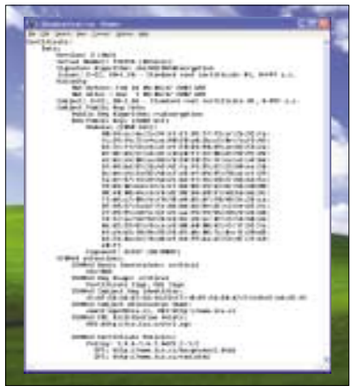
Bez notáře ani ránu

Pozornější z vás se možná po přečtení předchozí stati už už nadechují, že vám věšíme bulíky na nos. Pochopitelně máte pravdu: samotný certifikát jako takový ještě žádnou důvěryhodnost zvýšit nemůže. Stejně jako padělek vašeho pa-

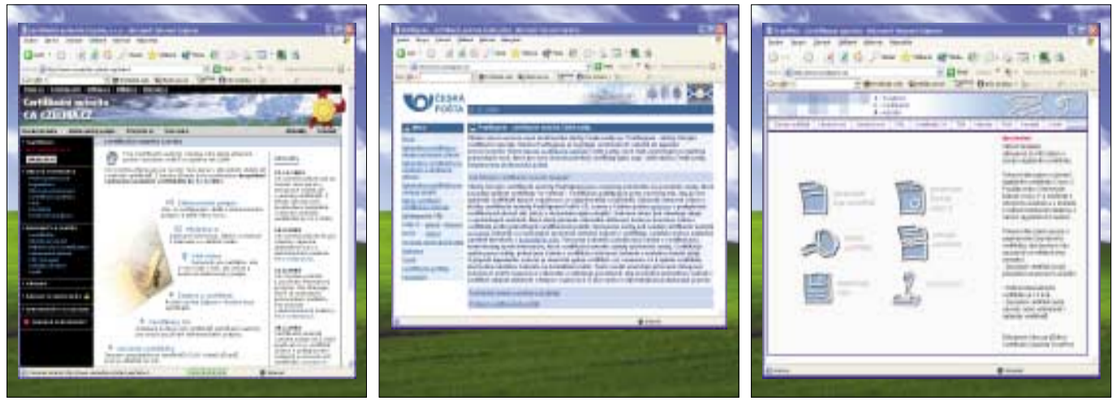








Ačkoliv může certifikát, zastoupený tradičním souborem, nabývat dle formátu či kódování různých podob, důležité je, že v sobě stále nese tutéž důležitou informaci: jedinečnou, nezaměnitelnou identifikaci držitele a nezpochybnitelný podpis „elektronického notáře", jenž identitu posvětil.



Komerčních certifikačních autorit, jež nabízejí širokou škálu služeb, je i na českém trhu celá řada. Nebojte se navštívit jejich stránky.

su či vysokoškolského diplomu bez příslušných razítek v nikom nevzbudí důvěru, ani „holý" certifikát komunikující protistranu nijak neuklidní. Je nasnadě proč: stejně jako zdařilý padělek občanky, i certifikát by dokázal „spíchnout na koleně" ledaskdo, takže jsme se nikam v důvěryhodnosti neposunuli. V pravou chvíli zde vstupuje do hry zcela zásadní instituce, již nazývá-

Stránky některých tuzemských certifikačních autorit

- *www.caczechia.cz*
- *www.c-a.cz*
- *www.trustport.cz*
- *www.postsignum.cz*

me velmi příznačně certifikační autorita. Její přirovnání k běžnému notáři je velmi přiléhavé a navíc dobře naznačuje, co je jejím úkolem. Certifikační autorita je oním důvěryhodným prostředníkem, jenž provádí zcela nezvratné a jednoznačné přiřazení existujícího certifikátu k jeho držiteli. Nejenže tento „elektronický" notář provede důkladnou kontrolu držitele certifikátu (ano, v případě nutnosti i kontrolu fyzickou!), ale též posvětí údaj z nejdůležitějších, a to již zmiňovaný veřejný klíč uživatele.

Aby tento princip fungoval v praxi, jsou nutné jisté předpoklady. Jedním z nich je, že oné autoritě (existují jich stovky) důvěřují obě protistrany, tedy že oba komunikující partneři se na svém „elektronickém notáři" shodnou jako na vyhovujícím. Druhým zásadním principem je, že elektronický notář musí opatřit vydaný certifikát jakýmsi nezvratným potvrzením, že pochází opravdu od něj. Jak se to děje? Hádáte správně, i zde se uplatňuje asymetrická kryptografie. Jenže jak? Já přeci nechci certifikát ukrýt, ale naopak zveřejnit a zároveň jednoznačně označit! Vtip spočívá v tom, že se použije postupu, jenž je znám jako digitální podpis (i o něm ještě bude řeč). Základní myšlenka je taková, že asymetrický klíčový pár se použije v opačném pořadí: vydaný certifikát je podepsán privátním (utajeným) klíčem certifikační autority, tento podpis je k certifikátu přiložen a jakýkoliv zájemce o prověření pravosti certifikátu může učinit kontrolu: nalezne na internetu veřejný klíč autority (a případně si jej uloží v operačním systému pro další operace), dešifruje její podpis a dospěje k výsledku, jenž mimo veškerou pochybnost potvrdí či vyvrátí pravost vydaného certifikátu. Zdá se vám to složité? Nebojte se, praktické příklady vše objasní názorně. Navíc uvedené operace pochopitelně z podstatné části provádí operační systém.

Kdo hlídá hlídače?

Budeme-li důslední, neuspokojí nás dokonale ani předchozí odstavce. Ano, certifikační autorita je důležitá věc, ale kdo kontroluje ji? Dobrá otázka, a stejně dobrá odpověď. Kontroluje ji jiná certifikační autorita. Vtip? Nikoliv, přesně takhle to funguje. Certifikační úřady (autority) totiž tvoří jakousi hierarchii, v níž nadřízený subjekt kontroluje toho pod sebou, a děje se tak zcela prakticky opět pomocí veřejných a privátních klíčů. Princip je prostý: každá autorita disponuje svým vlastním certifikátem, jenž je podepsán (a tedy zdůvěryhodněn) nadřízenou autoritou. A takhle to jde až...až kam? Až k autoritě, jejíž důvěra je tak silná, že už nadřízeného nepotřebuje. Je jí důvěřováno jaksi a priori, tedy na základě jiných kontrolních mechanismů. Tato autorita se označuje jako důvěryhodná kořenová (ačkoliv stojí na vrcholu – strom je zde vzhůru nohama) a její certifikát je podepsán – v souladu s logikou věci – jí samotnou.

Z mnoha důvodů je většina celosvětově uznávaných kořenových certifikačních autorit spojena s anglicky hovořící částí světa, takže studium jejich politiky a záruk je někdy obtížné. Ačkoliv české autority existují, vaši zahraniční obchodní partneři je asi znát nebudou.

Důvěryhodné kořenové autority plní mimořádně důležitou funkci. Jejich důvěryhodnost nesmírně usnadňuje praktické využití všech popisovaných struktur, neboť pravidlo zní: když důvěřuji kořenu, zároveň důvěřuji všemu, co on posvětil! Všechny podřízené autority jsou tedy důvěryhodné a všechny certifikáty těchto autorit také! A to je zásadní myšlenkový posun, jenž praxi výrazně zjednodušuje.

Celosvětově

- *www.verisign.com*
- *www.thawte.com*
- *www.entrust.net*

V tuzemsku

- *wwww.ica.cz*

Důvěryhodnost zblízka

Teorie je sice pěkná věc, ovšem co s tím vším? Naštěstí prostředí operačního systému Windows poskytuje dostatečné zázemí pro práci s certifikáty, a navíc běžně využívané aplikace umí rovněž tyto vymoženosti využít. V následující části článku si popíšeme praktické situace, na něž narazíte, a postupy, jichž se nemusíte bát. Jde přeci o vaši bezpečnost!

Prohlížíme certifikát

Už jsme toho o této struktuře namluvili až až, a ještě jsme žádný pořádný certifikát neviděli. Což se na něj tedy konečně kouknout? V prostředí operačního systému Windows to není žádným problémem, neboť systém dokáže standardní formáty certifikátů interpretovat do podoby přehledného grafického rozhraní, což práci značně usnadňuje.

Pro příklad jsme si vybrali certifikát, jímž je označena identita jednoho z veřejných webových serverů známé společnosti Symantec (byl tedy vydán pro počítač, ne člověka, to ale vůbec nevadí). Pokud jej otevřete, na kartě *Obecné* najdete základní údaje: v horní části účel certifikátu (v našem případě potvrzení identity vzdáleného počítače), v dolní části pak Vystavitele (autoritu, jež dokument vydala, zde zrovna seriózní VeriSign) a Platnost. Nepřehlédněte jeden zásadní detail – ikona v levém horním rohu není nijak označena, takže certifikát je považován systémem za důvěryhodný (viz další oddíl), a všechny aplikace mu tedy budou bezvýhradně věřit. Pokud by tomu tak nebylo, ikona by byla označena červeným kolečkem s křížkem a také varováním, že certifikát je vydán nedůvěryhodnou autoritou. Na další kartě *Podrobnosti* najdeme všechna pole certifikátu pěkně popořadě, bez výjimky. Všimněte si detailních údajů, z nichž vyjímáme např. Přístup k informacím úřadu, jež vás pomocí webové adresy přímo odkazují na vydavatele, takže si jej můžete „na vlastní oči" ověřit. Samozřejmě zde jsou také veřejný klíč držitele i popis postupu, pro který byl vytvořen (algoritmus pro šifrování). Neméně zajímavá je karta třetí s *názvem Cesta k certifikátu*, jež zahrnuje praktickou ukázku výše popisované hierarchie důvěryhodných autorit. Názorně zde vidíte, jak trnitá cesta může vést od kořene důvěry až ke konkrétnímu dokumentu, na nějž se díváme.

Vraťme se ještě na kartu *Obecné*, kde můžeme stisknout tlačítko *Prohlášení vystavitele*. Máte-li internetové připojení, rovnou se ocitnete na stránkách certifikační autority a jejího popisu tzv. politiky, na jejímž základě svou práci zastává. Zde také můžete pojmout důvěru (či nedůvěru).

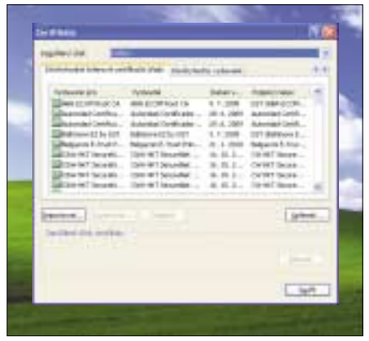
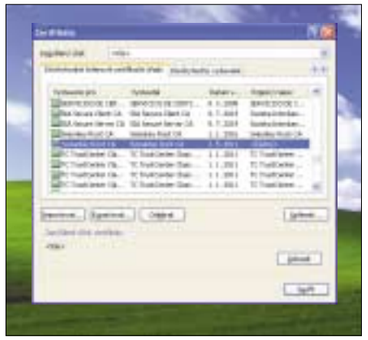
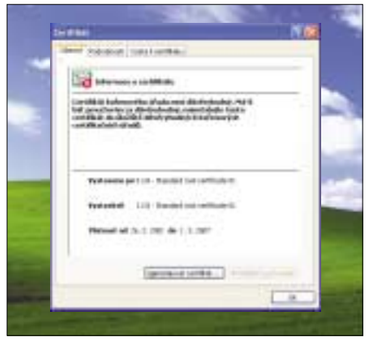
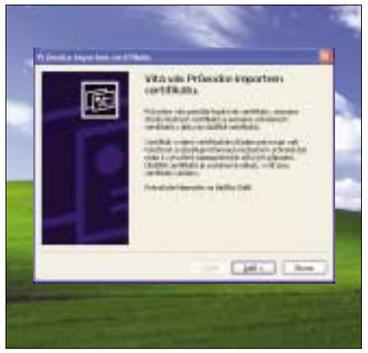
Které kořenové autoritě věřím?

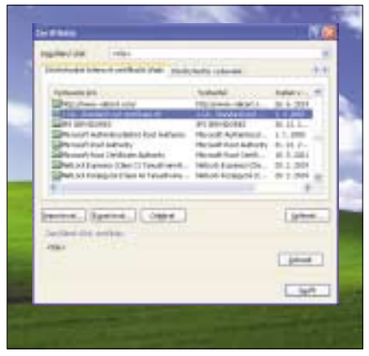
V předchozí části článku jsme si mimo jiné zdůraznili, že klíčový význam pro vyvolání důvěryhodnosti mají tzv. důvěryhodné kořenové autority. Tuto problematiku tedy prozkoumáme blíže, neboť nejde jen o holou teorii – operační systém Windows má v sobě totiž zakódováno pravidlo, že pokud nějakou autoritu označím za kořenovou a důvěryhodnou, pak jí slepě věří všechny aplikace a zbytečně se nevyptávají, Internet Explorerem počínaje a MS Outlookem konče. Pro uživatele je velmi cennou informací, že operační systém Windows ve výchozí podobě (tedy po instalaci) již mnoha kořenovým autoritám důvěřuje. Tedy, tvůrce systému Microsoft již základní kolekci autorit vybral za vás a snaží se vám práci usnadnit. Chcete-li mít věc pod kontrolou, je potřeba se na seznam alespoň podívat. Jedna z možností je využít ovládací panel *Možnosti internetu* (Internet Options), kde přejděte na kartu *Obsah*.

V prostřední části karty je pole *Certifikáty*, v němž použijte tlačítko *Vydavatelé...* a v následném dialogu přejděte na *kartu Důvěryhodné kořenové certifikační úřady*. Právě zde najdete seznam autorit, jež v tuto chvíli Windows (vaše Windows, tedy vy!) považují za důvěryhodné. V zásadě lze říci, že kolekce zahrnuje úřady, jimž lze i prakticky důvěřovat, takže seznam nemusíte nijak zásadně čistit. Na druhou stranu, chcete-li mít vše totálně pod kontrolou, prověřte všechny autority třebas dle informací na

Význam korektně uložených důvěryhodných kořenových certifikátů je pro řadu činností operačního systému a aplikací zcela zásadní. Například tvůrci antivirových programů využívají ověření pravosti svých automatických updatů právě pomocí certifikátů, a jejich absence by mohla činnost aplikace narušit. Dobrým příkladem je třeba služba Live Update firmy Symantec, jejíž certifikát vidíte na obrázku mezi ostatními důvěryhodnými kořenovými certifikáty.

K přehlednému zkoumání certifikátů nabízí operační systém Windows jednotné, dobře použitelné rozhraní. Veškeré údaje jsou k dispozici na jednom místě, a navíc lze provádět i exporty či další operace.



Do seznamu kořenových certifikátů důvěryhodných autorit se ve Windows můžete dostat různými cestami, avšak vždy platí, že pracujete s jediným, centrálním úložištěm, jen v různých pohledech. Nezapomínejte, že jde o sídlo vaší automatické důvěryhodnosti!

internetu a podezřelé či neznámé prostě vymažte. Mimochodem, kontrolní otázka: čím jsou kořenové autority reprezentovány? Správně, svými certifikáty! Chcete-li si je prohlédnout v detailu, označte jakoukoliv položku v seznamu a použijte tlačítko *Zobrazit*. Mezi zařazenými certifikáty naleznete např. autority, jako jsou VeriSign či Thawte, o jejichž serióznosti opravdu nemusíte pochybovat.

Často však může nastat situace, že seznam položek nebude pro vaše účely dostačovat. Co může být důvodem? Váš obchodní či jiný komunikační partner může zkrátka využívat služeb jiné autority, jejíž důležitost nebyla pro společnost Microsoft dost vysoká na to, aby byla přímo zařazena. Proto si potřebný certifikát do seznamu přidáme.

Řekněme, že kýženou autoritou je tuzemská I. CA, jejímž zřizovatelem je dceřiná společnost známé PVT. Té můžeme v našich podmínkách věřit, což navíc stvrdily i státní instituce uděleným speciální akreditace. Jak ji zařadit do seznamu, aby ji všechny aplikace rovnou považovaly za seriózní?

Prvním krokem je získání jejího certifikátu z internetu. Po vstupu na domovskou stránku *www.ica.cz* najdeme ihned v obrázku odkaz s názvem Certifikát certifikační autority, a při použití odkazu se ocitneme na stránce se soubory ke stahování. Můžete zvolit druhou či třetí položku v seznamu a využít tlačítka *Instaluj*, čímž spustíte uložení certifikátu na pevný disk. Protože přípona „.cer" je operačním systémem rozpoznávána, soubory jsou opatřeny nazelenalou ikonkou a v případě, že na ně poklepete myší, dojde k jejich otevření v typickém okně. Můžeme si ověřit všechny potřebné údaje a také pomocí indikátoru zjistíme, že certifikát je vydán společností, které v tuto chvíli ještě nedůvěřujeme, což je v pořádku – celou operaci přeci provádíme, abychom to změnili!. Chceme-li to zařídit, použijeme volbu *Nainstalovat certifikát...*, čímž jej zařadíme do dříve zkoumaného seznamu, jak je patrné na následujícím obrázku.

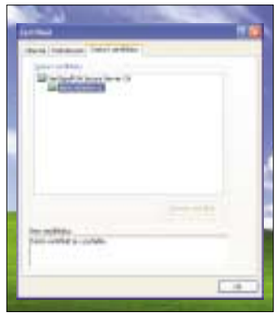
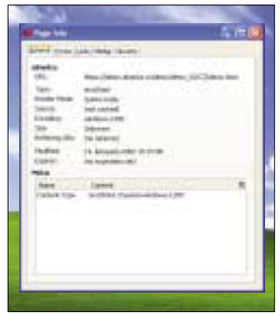
Čeho jsme dosáhli? Od této chvíle budou všechny aplikace v našem systému automaticky věřit této nové autoritě a všem certifikátům, jež ona vydala. Nikdo se vás na to už nebude ptát – bude-li cokoli podepsáno od I.CA, systém to prostě přijme. Budete-li to chtít v budoucnu změnit, nezbývá než certifikát kořenové autority ze seznamu odstranit.

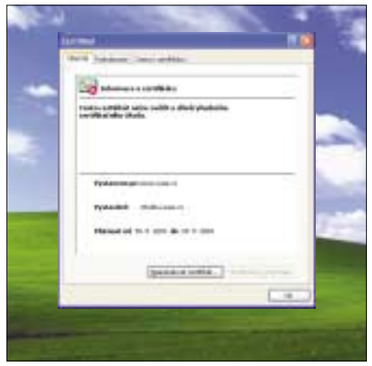
Web, kterému mohu věřit

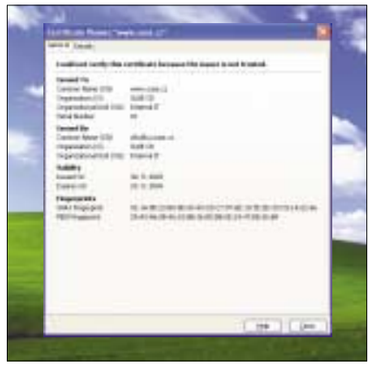
Jedním z nejdůležitějších způsobů implementace ověřování pomocí certifikátů je zajištění důvěryhodnosti webových serverů, jež poskytují uživatelům své webové stránky. Bez této technologie je prakticky nemyslitelné nakupování na internetu či nahlížení do tajů vlastních bankovních účtů, telefonních poplatků atd. Naším cílem je tedy především zjistit, zdali na druhém konci internetu je opravdu naše banka, náš telefonní operátor či náš obchodník. Proč? Protože se prakticky vždy při takovýchto transakcích připojujeme přihlašovacím jménem a heslem, a musíme si být jisti, že jsme je nezaslali nějakému podvodníkovi.

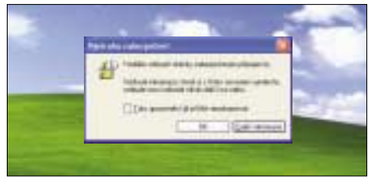
Praktickou realizací výše popsaných nároků je všeobecně rozšířená dvojice protokolů SSL a TLS. Netrapte se názvy, vše si předvedeme názorně. Prvním krokem je vstup na inkriminovanou webovou stránku, jež vám nabídne svou identifikaci za účelem získání důvěry z vaší strany (její název bývá uvozen pomocí „https"). Jako příklad jsme využili stránky eBanky, jež u nás patří v oblasti zabezpečené komunikace klientů mezi průkopníky. Při snaze o vstup na webový server, jenž se prokazuje certifikátem, vás prohlížeč upozorní, že se tak děje, pomocí dialogu (viz obrázky). Poté dojde k běžnému zobrazení webové stránky, avšak s jedním rozdílem: na pozadí již probíhá šifrovaný přenos a server vám zaslal svůj certifikát, o jehož pravosti se můžete (přesněji řečeno byste se měli) vždy přesvědčit! Kde jej najdete? V Internet Exploreru se ukrývá vpravo na dolním panelu v podobě ikony se zámkem, prohlížeč Mozilla (resp. Firebird) jej prezentuje v levém dolním rohu okna pod velmi obdobným obrázkem. Předtím, než na takto zabezpečenou stránku vstoupíte, měli byste se ujistit o její serióznosti. V zásadně můžete postupovat dvěma cestami: budete spoléhat na kořenové autority a tím i na podřízené certifikáty, nebo si skutečně každý certifikát prohlédnete. V případě námi předváděné eBanky obdržíte zobrazení (viz obrázky), jež potvrzují, že vše je v pořádku: certifikát je v období platnosti a vydavateli, společnosti VeriSign, důvěřujeme.

Co by nás mělo odradit? Jednou z věcí, na níž dávejte pozor, je pochopitelně podpis důvěryhodné certifikační autority. Jak se projeví jeho případná absence? Pokud vstoupíte na stránky, jež jsou vybaveny certifikátem, o němž operační systém nic neví, prohlížeč vás bude vždy varovat (viz obrázky).

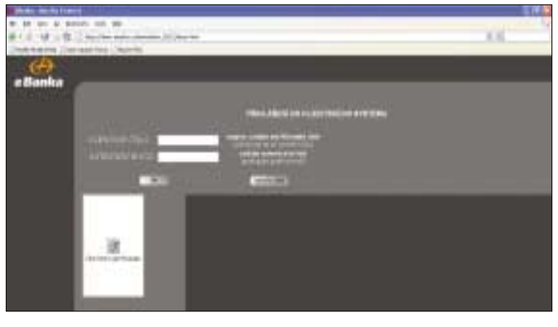





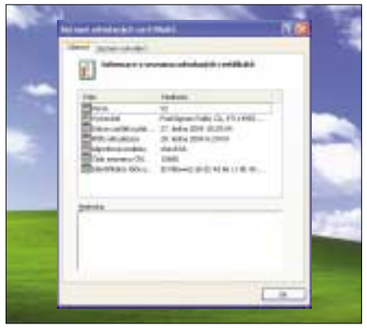
Pokud váš prohlížeč při přístupu na zabezpečenou stránku ohlásí nějakou nesrovnalost, zběžné prohlédnutí certifikátu by mělo být samozřejmostí. K dispozici je opět standardní náhled, jako v jiných případech.

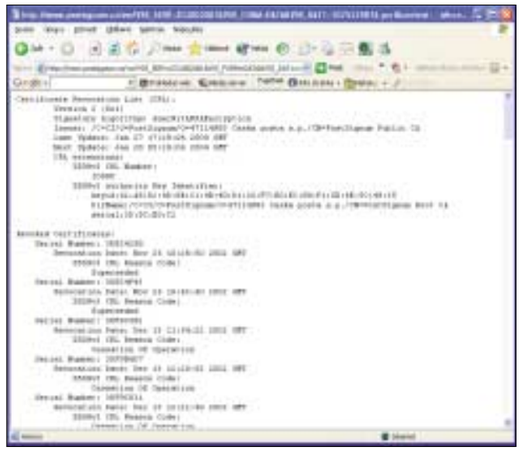


Při prácí s jakýmkoliv certifikátem (bez ohledu na to, zda je vydán pro uživatele, počítač či přímo autoritu) byste měli krom kontroly identifikačních údajů ověřovat především to, zda je certifikát momentálně platný (nevypršela jeho životnost), zda byl vydán pro vás důvěryhodnou autoritou, dále zda váš komunikační protějšek se jmenuje stejně, jako oprávněný držitel certifikátu (platí pro člověka i počítač), a na závěr zda nebyl certifikát odvolán. Pochybnost v kterémkoliv z těchto zásadních parametrů by ve vás měl vyvolat oprávněnou nedůvěru a vést alespoň k prověření těchto skutečností nezávislou cestou.

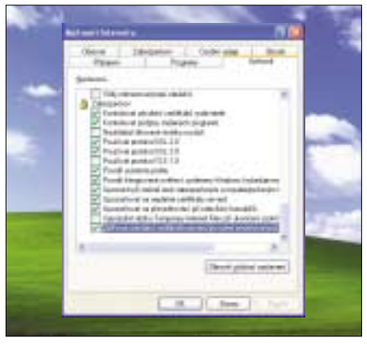
Za příklad jsme si zvolili stránky tuzemského zastoupení společnosti SuSE: její webová aplikace využívá jako autoritu vlastní úřad, realizovaný firmou SuSE, a tento certifikát není podepsaný žádnou nadřízenou, světově uznávanou autoritou. Při detailním prohlédnutí takového certifikátu na to budete důsledně upozorněni a prohlížeč vás výslovně vyzve, abyste buďto riziko přijali, nebo přístup odmítli. V případě, že požadujete vysoce důvěryhodný přístup (heslo do banky, číslo kreditní karty), nikdy byste neměli toto podcenit a raději kontaktujte protistranu s dotazem, proč k této situaci došlo.

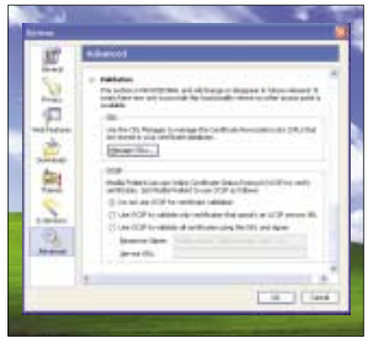
Riziko je totiž nasnadě: pokud by si hypotetický podvodník vytvořil kopii webových stránek firmy SuSE a úspěšně předstíral identitu falešným certifikátem, budete sice posílat svá citlivá data zašifrovaně, ale přímo do rukou útočníka! Druhou věcí, jež by vás měla odradit, je časová neplatnost certifikátu. Tuto skutečnost opět prohlížeče hlásí uvedeným způsobem, a pokud je na straně webového serveru certifikát opravdu „prošlý“, žádnou citlivou transakci rozhodně neriskujte.





Dostupnost všech informací o odvolaných certifikátech je základním opěrným bodem celé struktury důvěryhodnosti. Tato fakta můžete ověřovat jak přímo nahlédnutím do seznamu CRL, tak pomocí funkce vzdáleného ověřování, již dovedou běžné prohlížeče provádět.





Není certifikát odvolán?

V dosavadním textu jsme si již mnoho pověděli o prověření správnosti a důvěryhodnosti certifikátů, avšak přesto jsme jeden zásadní aspekt prozatím vynechali, takže pojďme blíže k němu. Tak jako certifikační autorita certifikáty vydává, tak je čas od času také odvolává neboli revokuje.

Důvody mohou být různé: uživateli zhavaruje systém a klíčový pár je ztracen, někdo případně zcizí notebook s klíčem i certifikátem, nebo vyjdou najevo skutečnosti, jež důvěryhodnost klienta zpochybní. V podobných případech je autorita nucena okamžitě říci, že takový certifikát neplatí, aby se tímto všichni mohli řídit. Možná se ptáte, kde je problém? No právě v tom, že z dříve vydaného certifikátu se nepozná, že byl odvolán! Je-li jakoby stále platný a autorita je důvěryhodná, není se zdánlivě čeho obávat. Pokud se však v té době již certifikát dávno nachází na seznamu odvolaných (tzv. revocation list), je jakákoliv důvěra vrcholným hazardem.

Co s tímto v praxi? Každá solidní autorita seznam odvolaných certifikátů uveřejňuje, takže je možno do něj nahlédnout. Ovšem detailní kontrola každého certifikátu dohledáváním v rozsáhlých seznamech je pochopitelně neúnosná, i když možná – proto například MS Internet Explorer tuto funkcionalitu implementuje, a pokud ji aktivujete, provede ověření za vás. Tuto možnost rozhodně nepodceňujte a vždy ji mějte zapnutou.

Potřebná nastavení najdete v MSIE opět v dialogu *Možnosti Internetu*, na kartě *Upřesnit*, úplně na dolním konci seznamu jako položku Zjišťovat odvolání certifikátů serverů. V prohlížeči Mozilla pak hledejte v menu *Tools/Options* položku Advanced a opět seznam odrolujte na dolní konec. Zde můžete buďto zapnout používání protokolu OCSP, jenž vše zařizuje po síti, nebo ručně naplnit seznamy odvolaných certifikátů přímo v operačním systému. Jak takový seznam odvolaných certifikátů (Certificate Revocation List) vypadá, se můžete podívat na obrázku.

Pokračování příště

Náš miniseriál v tomto místě prozatím ukončíme. Dnes jsme si vysvětlili, jak celý systém funguje a jak se chovat především v případě, že na druhé straně komunikace se nachází webový počítač, jenž dokazuje svou totožnost. V příštím dílu se zaměříme na certifikáty uživatele – osoby, blíže nahlédneme k práci s e-maily a prakticky si ukážeme šifrování pošty a její digitální podpis.

4 0112/FEL ❑