Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 4/2004 **15. duben 2004**

4/2004

Připravil : Mgr.Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(529 registrovaných odběratelů)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Novela zákona o elektronickém podpisu a časové razítko

Doc. Ing. Vladimír Smejkal, CSc.

U čtenářů Crypto–Worldu lze snad právem přepokládat, že vědí, co to je a na jakých principech funguje časové razítko; proto se budu věnovat pouze některým konsekvencím novinky, která je v současné době začleňována novelou zákona o elektronickém podpisu do naší legislativy.

V poslední době bylo u nás časové razítko poněkud démonizováno, neboť se objevily názory, že elektronický podpis bez časového razítka není dostatečně věrohodný, bezpečný, nezneužitelný apod. Není tomu tak, neboť ve skutečnosti existuje velice málo právních úkonů, kdy by byly rozhodujícími hodiny, minuty či dokonce sekundy. Na druhou stranu je ale třeba říci, že dnes poněkud extrémním požadavkům na bezpečnost a věrohodnost automatického zpracování dat (které již mnohonásobně převyšují požadavky, ale i reálné záruky „klasického“ zpracování na papíře), může možnost opatření elektronického dokumentu časovým razítkem vyhovovat.

V právu Evropských společenství byla otázka novely Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (dále jen „Směrnice“) také zvažována, ale nakonec bylo konstatováno, že jde o komerční záležitost, která je předmětem nabídky a poptávky, ale kterou není třeba žádným způsobem kodifikovat, či dokonce vyžadovat.

To, že ČR se přesto rozhodla časové razítko kodifikovat, je možná způsobeno přehnaně pozitivistickým vnímáním legislativy resp. práva jako takového u nás, možná je to důsledek stále se více prosazujícího trendu, vnímat právní normy současně i jako normy organizační či jako jisté standardy. Ale v tomto případě to zřejmě nebude na škodu.

Novela zavádí tzv. „kvalifikované časové razítko“, což je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Nutno říci, že teprve při psaní tohoto článku jsem si uvědomil jistou past doslovného výkladu této definice, která pravděpodobně vychází z nějakého zahraničního dokumentu, tvořeného technology (zřejmě ze standardů ETSI a doporučení RFC 3161). Lze totiž diskutovat o tom, jak dlouho data existovala před daným časovým okamžikem. Možná by bylo přesnější použít definici jinou, právnicky přesnější, tj. typu „data existovala v okamžiku doručení otisku (hash) dokumentu (k němuž je časové razítko vyžadováno) k poskytovateli“. Ale toto může být dle mého názoru řešeno výkladově.

Pojem „kvalifikovaný poskytovatel certifikačních služeb“ zní sice nově, ale jedná se v podstatě do zákona vloženou legislativní zkratku pro osobu, která vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen „kvalifikované certifikační služby“) a splnil ohlašovací povinnost Ministerstvu informatiky podle § 6 zákona.

Kvalifikovaný poskytovatel certifikačních služeb (dále také jen „poskytovatel“), který vydává kvalifikovaná časová razítka, je povinen podle novely zákona:

a) zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem,
b) zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,
c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,
d) přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,
e) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

Zákon říká v novém § 6b odst. 2, že kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání. Tady samozřejmě očekávám stejné námitky rádobypuristů a technologických vykladačů práva (jako jsou např. ti, kdo neumějí vyložit pojem „oblast orgánů veřejné moci“), co že to je ono „neprodleně“, a je mi jasné, že budou požadovat kvantifikaci, nejlépe s přesností na milisekundy. Neprodleně znamená tak nejdříve, jak je to možné – viz také předchozí připomínka o okamžiku existence „razítkovaných“ dat.

Osobně se domnívám, že stejně bude muset být novelizována prováděcí vyhláška č. 366/2001 Sb., tedy je možné v novém znění uložit poskytovatelům časových razítek povinnost, aby do svojí „razítkovací“ prováděcí směrnice napsali, jakou dobu odezvy a přesnosti časového údaje zaručují. Případně by vyhláška mohla specifikovat, zda ukládaným časem ve smyslu písm. b) výše je čas vytvoření otisku dokumentu (to asi nevíme resp. nemůže být zaručeno), doručení žádosti obsahující hash dokumentu k poskytovateli, nebo nejbližší možný čas poté (tj. ono neprodleně). Zákon v novém § 12b říká, že časové razítko má obsahovat hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka; existuje ovšem drobné riziko následující:

1. mějme žadatele A s dokumentem D, který požádá o přiřazení časové značky odesláním žádosti na TSA_A, kam je tato žádost doručena v čase T_1;
2. mějme žadatele B s stejným dokumentem D, který požádá o přiřazení časové značky odesláním žádosti na jinou TSA_B, kam je tato žádost doručena v čase T_2;
3. čas T_2 je pozdější, nežli čas T_1 ($T_2 > T_1$); oba časy se ale odlišují minimálně (na rozlišovací úrovni technického zařízení) $T_2 \rightarrow T_1$;
4. čas, který je vygenerován do razítka, je pro žadatele A: $T_A = T_1 + t_a$, pro žadatele B: $T_B = T_2 + t_b$;
5. pokud je doba odezvy (vygenerování časového razítka) t_b u TSA_B kratší nežli doba odezvy t_a u TSA_A, tj. $t_b < t_a$, pak se může stát, že bude současně platit $T_2 > T_1$ a $T_A > T_B$; jinými slovy, čas vztahující se k dokumentu D doručenému dříve na TSA_A bude pozdější, nežli čas vztahující se k dokumentu D doručenému později na TSA_B. Stane se tak v případě, že $T_1 - T_2 \geq t_b - t_a$.

Možná bude někdo považovat tento příklad za umělý. Zas tak umělý mi nepřipadá, neboť si dovedu představit situaci, kdy je dokument D osobou B odcizen osobě A, jež je autorem vynálezu, v dokumentu popsaném). A vnímaví čtenáři jistě přijdou i na jiné možnosti.

B. Jak jsem pochopil ochranu informace, část 3
RNDr. Antonín Beneš, PhD., KSI MFF UK Praha

Chtěl bych dnes začít něčím novým, ale nedá se nic dělat, zůstaneme ještě chvíli u normosloví. Je to možná otravné, ale zato nám to pomůže lépe projít kardinální otázku celé bezpečnosti, totiž tvorbu globální bezpečnostní strategie, které se obvykle říká bezpečnostní politika. To, že je pojednání o standardech neorganicky přestřiženo v půli mohu přičíst vlastní rozvláčnosti, nebo se mohu vymlouvat na šéfredaktora, který je pes a nedá mi více jak čtyři strany.

Minule jsem se zabýval technickými, až technologickými normami bezpečnosti. Už jsem naznačoval, že bezpečnost je spíše proces, než stav. Že to ani tak není v technice, kterou si nakoupím, jako spíše v jejím správném používání. To mne ovšem nutí povědět něco o normách, které bych označil jako organizační. Jako již tradičně, je jich více. My se za všechny podíváme na normu ve své kategorii nejpopulárnější - BS7799

BS 7799 - britská kvalita

Jednoduše řešeno žádná z tzv. organizačních norem neříká, nic o tom, jak konkrétně by měl vypadat váš bezpečnostní mechanismus. Žádným způsobem z nich nelze ani odvodit, jaké mají být vlastnosti implementovaného bezpečnostního opatření, či zda vůbec máte něco implementovat. BS 7799, ISO IEC TR 17799, či jak se tato norma různě jmenuje není výjimkou. Přesto je mimořádně užitečná.

Ona totiž říká, jakým způsobem máte bezpečnost dělat. Stručně řečeno, dozvíte se zde, že máte postupovat shora dolů, tj. začít od bezpečnostní politiky a tu postupně rozvést až na úroveň implementace jednotlivých protiopatření. V té nejhrubší formě vás BS7799 nabádá, abyste se zabývali následujícími okruhy problémů:

- bezpečnostní politika
- klasifikace a řízení aktiv
- personální bezpečnost
- fyzická bezpečnost a bezpečnost prostředí
- řízení provozu a komunikací
- řízení přístupu
- vývoj a údržba systémů
- řízení kontinuity operací
- soulad s požadavky (právní, technické, audit)

Jinými slovy, BS7799 vám neřekne, že si máte koupit takovou či makovou zálohovací knihovnu. Namísto toho vás upozorní, že si - mimo jiné - máte rozmyslet, co, jak a proč chcete ve svém systému zálohovat. Norma tedy slouží jako jakýsi seznam, který si můžete odškrtat. Podobně jako při balení kufru, na konci budete mít jistotu, že se na nic důležitého nezapomnělo.

Pro úplnost bych měl ještě dodat, že pro podporu budování bezpečnosti podle metodiky, kterou zavádí BS7799 byl vytvořen automatizovaný nástroj CRAMM. Ten můžete pokrmit seznamem svých aktiv, jejich hodnoty pro vás a jejich vzájemných souvislostí. On zhodnotí vstupy, pohrabe se ve své databázi opatření a vydá víceméně srozumitelné

doporučení, jaká bezpečnostní opatření byste měli aplikovat. Bible i CRAMM mají cosi společného - správný výklad jejich tvrzení dělá divy.

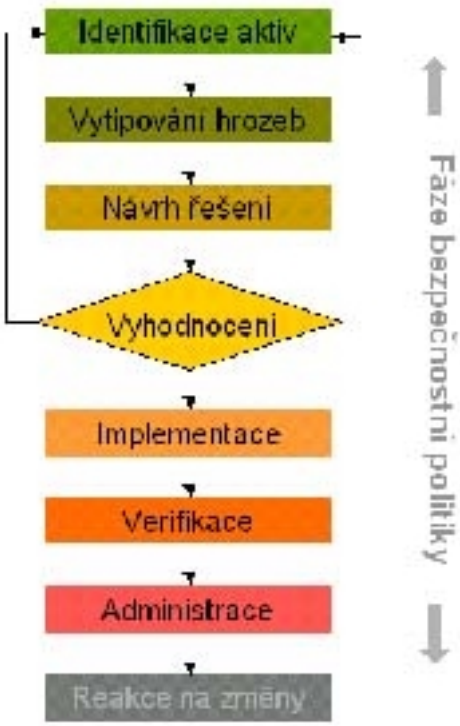
Vzhůru do (bezpečnostní) politiky

Nyní již jste dostatečně vybaveni teorií na to, abyste mohli začít plánovat svoji bezpečnost. Před tím, než se pustím do klasického výkladu, jak činit bezpečnostní politiku, neodpustím si několik poznámek, kterými se Vás pokusím varovat před realitou světa a uvedu na pravou míru několik mylných názorů.

Tak předně, není pravda, že bezpečnostní politika je jen "pro ty velké". Dále není pravda, že bezpečnostní politika je obrovské množství práce na celé měsíce. A už vůbec není pravda, že by bezpečnostní politika nic neřešila. Na druhou stranu také není pravda, že vaše bezpečnostní politika musí být zcela jedinečná a šitá od počátku na vás.

Je to všechno otázka míry. Diplomat zvažuje, zda nesouhlasit nebo vyjádřit politování, vy spíše jak zakamuflovat pozdní příchod domů. Nezvládnutí vede v obou případech ke zvýšenému napětí. Bezpečnostní politika vám říká, jak zvládnout problém zajištění IS proti incidentům. Když to nezvládnete, budete mít problémy. Všimněte si, že nezávisle na velikosti organizace problémy budou vždy - vzhledem k svému "majiteli" - velké.

Zatímco nadnárodní korporace bude mít patrně stovky stran bezpečnostní politiky a souvisejících předpisů, váš třichlapový "bussiness" vystačí ke stejnému účelu s nepoužitou stranou účtenky, kam se poznačí, že Franta nastaví heslo pro roota a Honza přestane válet smlouvy po celé kanceláři. Důležitější než rozsah je, aby pokrývala všechny důležité okruhy problémů formou, která je srozumitelná všem, kterých se týká. Její smysl je v tom, že vám umožní rozmyslet si, kde vás bota tlačí a naplánovat si řešení. Tady ale pozor. Viděl jsem příliš mnoho projektů, kde se celé měsíce mapovalo, plánovalo, ladilo a výsledkem byl několika set stránkový materiál. Ten materiál popisoval neexistující systém, protože zkoumaný IS se v průběhu zkoumání vyvíjel, což nebylo možné zohlednit, protože jinak by dokument nikdy nebyl dopsán. Nikdo jej nikdy nečetl, protože to bylo moc složité a neaktuální. A taky už nezbyly prostředky na rozsáhlá bezpečnostní opatření, která dokument navrhoval. Uživatelům nařídili změnit si heslo, koupil se firewall, IDS, certifikační autorita nebo něco podobného a bylo vymalováno.



Nebojte se při vymýšlení bezpečnostní politiky koukat k sousedům. Zejména organizace pohybující se ve stejné branži budou mít podobné nároky na bezpečnost a tudíž budou aplikovat podobná opatření. Není nutné hned vytvářet plagiáty, stačí se inspirovat.
Dost ale bylo strašení, pojďme se podívat, jak se taková bezpečnostní politika vytváří.

Jak na to

Na úvod můj oblíbený obrázek ukazující životní cyklus bezpečnostní politiky a šířeji celého

bezpečnostního mechanismu. Pozornosti doporučuji zejména vzhůru vedoucí šipky, které pozorovatele vracejí tak říkajíc na začátek. To je přesně to, co dělá z bezpečnostní politiky použitelnou bezpečnostní politiku a z bezpečnostních mechanismů užitečné bezpečnostní mechanismy. Už jsem říkal, že bezpečnost je proces. Bez soustavného přizpůsobování se změnám vnějšího prostředí a vývoji vlastního IS je to celé k ničemu a energie, kterou jsme vynaložili je ztracená.

Identifikace a odhad aktiv

Základem je zjistit, co vlastně ve svém informačním systému mám a k čemu je to dobré. Zdánlivě triviální zadání nabývá nového rozměru u organizací s tisíci zaměstnanci. Nezřídka se ukáže, že nikdo neví, kde fyzicky server leží, jak se zapne, co dělá ta modrá krabice v rohu, k čemu je dobrá komponenta XY. Ještě složitější bývá zjistit, co se stane, když ten který kus přestane fungovat.

Přesnější výsledek docílíme sčítáním po jednotlivých kategoriích, např.

- hardware - počítače, monitory, pásky, tiskárny, disky, komunikační media, …
- software - operační systém, koupené programy, vlastní zdrojové kódy, knihovny
- data - vlastní uložená data, logy, archivní kopie, listingy, …
- lidé - pracovníci potřební k správnému chodu systému, správci, programátoři
- dokumentace - programů, technického vybavení, systému, administrativní postupy
- spotřební materiál - papír, diskety, tonery, pásky do tiskáren, …
- ... atd. Zjevně každý si musí vymyslet vlastní seznam.

V podstatě v tomto kroku provedeme zevrubnou inventarizaci celého systému. Cena některých částí může být pouze velmi přibližně odhadnuta a i takový odhad může být velmi obtížný.

Určení hrozeb

Toto je další dosti záludný krok. Je potřeba určit, co nás bude stát realizovaný bezpečnostní incident. Nejlépe se o věci přemýšlí tak, že zkoumáte, kolik vás bude stát náprava (nové pořízení) a o kolik přijdeme (tj. kolik nevyděláme), než budou věci opět v richtiku. Chce to trochu vynalézavosti. Za kolik si pořídíte nové železo je jasné, mírně složitější je, za kolik si pořídíte novou dobrou pověst seriózní firmy s dlouholetou tradicí, ale i toto lze vcelku jednoduše vyčíslit. Trochu horší bude zjistit, kolik bude stát, když konkurence získá náš tajný návod na výrobu té nejlepší slivovice.

Hrozby, které musíte zvážit zahrnují nejméně:

- dopad přírodních katastrof - požár, vichřice, záplavy, výpadky napájení, selhání techniky
- poškození třetími osobami - přístupy po síti, vytáčená spojení, hackeři, kolem-jdoucí, lidé zkoumající odpad firmy
- následky zlomyslných pracovníků - zklamaní pracovníci, úplatkářství, zvědavci
- důsledky neúmyslných chyb -

Dotazníček			
Hodnota	***Utajení***	***Integrita***	***Dostupnost***
Hardware		přetížení, zničení, poškození	
Software	odcizen, kopírován	modifikován	smazán, přesunut
Data	zpřístupněna vně firmy	zničena chybou SW ; HW ; lidí	smazána
Lidé			únava, nemoc
Dokumentace			ztracena, odcizena
Materiál			odcizen, zničen

zadání špatných příkazů, vadných dat, skartace špatných dokumentů, kompromitace tajných materiálů

- ... a asi tisíc dalších

Zjišťování těchto faktů lze provádět formou dotazníku, který vyplní zainteresovaní pracovníci (viz. obrázek).

Odhad pravděpodobnosti zneužití

Když už víme, jaký dopad by měla realizace té či oné hrozby, je třeba zjistit, jak často dojde ke zneužití některé z expozic systému. Učinění těchto odhadů může být velmi obtížné, zkuste říci, jaká je pravděpodobnost, že vyhoříte. Trochu pomáhá přemýšlet o věci nikoliv jako o pravděpodobnosti, ale jako o četnosti. Jak často mi někdo ukradne šrajtofli, jak často se ztratí myš, jak často praskne stoupačka a vyplaví serverovnu. Když ani toto nepomáhá (jak často přijde do Prahy tisíciletá voda), lze použít některou z následujících metod:

- Odhad na základě obecných dat - např. pojišťovny mají rozsáhlé záznamy o počtu katastrof a o průměrných způsobených škodách, o počtu vloupání, podvodů. Výrobci mají přehled o životnosti a počtu selhání zařízení, …
- Odhad na základě vlastních dat - za dobu činnosti firmy vzniklé záznamy o závadách zařízení, počtech vadných loginů, …
- Bodovací systém počtu výskytů události – např. dle tabulky v rámečku čímž se snažíme vytáhnout z vlastních lidí i to, co nevědí. Na druhou stranu, kdo jiný by měl vědět víc o vlastním informačním systému
- Delfská metoda - okruh hodnotitelů provede hodnocení dané veličiny. Poté je každý seznámen s výsledky ostatních a upraví své hodnocení. Pokud jsou upravená hodnocení podobná, máme výsledek, v opačném případě výsledek vznikne dohodou hodnotitelů.

Výpočet očekávaných ročních ztrát

Pokud jsme si určili odpovědně pravděpodobnost (četnost) výskytu incidentů a jejich dopady, bude výpočet očekávané ztráty již jednoduchý. Stačí prostě vynásobit odpovídající dopady a pravděpodobnosti a vše sečíst. V tomhle místě se však ukáže jistá slabina metody. Nadhodnocení dopadů a četností může vést ke zcela nesmyslným odhadům ztrát, takže výsledek je potřeba opatrně podrobit posouzení selským rozumem. Tento krok je do značné míry kritický, neboť je obtížné poradit, jak poznat nesmyslný výsledek od správného, leč překvapivého. Trochu pomůže zkušenost.

Frekvence	*Hodnocení*	*Frekvence*	*Hodnocení*
více než 1 x za den	10	1 x za měsíc	5
1 x za den	9	1 x za 4 měsíce	4
1 x za 3 dny	8	1 x za rok	3
1 x za týden	7	1 x za 3 roky	2
1 x za 2 týdny	6	méně než 1 x za 3 roky	1

Kvalifikovaný odhad ztrát bývá často vyšší, než se obvykle předpokládá. To není nutně na škodu, neb tak lze problému ochrany zajistit potřebnou pozornost. Rovněž je možné po analýze toho, kde se ztráty berou, vytyčit okruhy bezpečnosti, kterým je třeba se věnovat přednostně.

Postprocessing

Poté, co jsme si v čistě technokratickém počítání zjistili, jaké jsou naše problémy, je třeba najít odpověď na následující okruhy otázek:

- Jaké právní normy chrání utajení a integritu dat?
- Jaké další normy je nezbytné dodržet?
- Co nás bude stát, pokud se na shora uvedené skutečnosti nebudeme brát ohled.

Vím, že by se zákony měly dodržovat, ale když jde o peníze, musí zhusta city stranou.

Přehled použitelných ochranných mechanismů

Pokud vyčíslený odhad ztrát je příliš vysoký, je třeba zavést nové ochranné mechanismy. Ne nutně dojdeme k tomuto výsledku, ale pokud někdo zjistí, že ztráty jsou zanedbatelné a nebude mít chybu ve výpočtech, musí udělat pouze jedinou věc - dát mi vědět. Bude první, o kterém jsem slyšel.

V opačném případě je na čase něco začít s bezpečností dělat. Můžete probrat jednotlivé expozice systému a zkoumat možnosti jejich pokrytí, nebo naopak mezi všemi ochrannými mechanismy hledat nějaký, který by řešil náš problém. Počítání od výsledku není až tak nesmyslné, uvažte, že stejně nevyrazíte ze svého IS nic, co by sám od sebe neuměl. Naopak, pokud v sobě nějaké bezpečnostní mechanismy má, je na čase zamyslet se nad jejich použitím.

Výsledkem je, zcela nečekaně, seznam navrhovaných opatření.

Nástin ročních úspor ze zavedení ochranných mechanismů

S bezpečností je jeden problém - nic užitečného to nedělá, ani to není zelené, ani to neposkakuje rozverně po obrazovce. Jak tedy přesvědčit manažery, že je třeba do toho investovat, nedejbože se tím zabývat, ještě ke všemu soustavně. Co s tím?

Můžeme spočítat, o kolik se sníží odhad očekávaných ztrát. Víme, jaká je cena zavedení nových ochranných mechanismů, znovu vyčíslíme očekávanou ztrátu po zavedení těchto opatření a rozdíl těchto hodnot lze prezentovat jako odhad celkových úspor. Slovo úspora slyší každý manažer rád a když se nám ještě podaří, že úspora je nezáporné číslo, bude to úplně prima.

Na závěr tradiční domácí úkol: připravte si pro svého šéfa pět důvodů, proč investovat do bezpečnosti. Zkuste ho přesvědčit, že alespoň jeden z nich je dobrý.

C. Kryptografie a normy - Digitální certifikáty

Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), část 4.

Jaroslav Pinkava, PVT a.s.

1. Úvod

Vracíme se k dokumentu ETSI 102158 (lit. [1]), a pokračujeme v popisu požadovaných vlastností politiky atributové autority. V minulé části bylo hovořeno o problematice životního cyklu podpisového klíče AA a o administrativních a řídících procedurách AA.

2. Řídící procedury AA (operační management)

Atributová autorita musí zajistit, že systémy AA operují bezpečně a správně, s minimálním rizikem poruch. Konkrétně:

- integrita systémů AA a informací musí být chráněna proti virům, a proti neautorizovanému softwaru a softwaru, který má za cíl poškodit systém;
- škoda vzniklá při bezpečnostních incidentech musí být minimalizována užitím příslušných reportů a procedur;
- použitá media musí být chráněna před poškozením, zneužitím a krádeží;
- musí být ustaveny a implementovány postupy pro všechny důvěryhodné a administrativní role, které ovlivňují poskytování certifikačních služeb.

S použitými medii musí být pracováno podle požadavků, které jsou kladeny v rámci schématu klasifikace informací. Média, která obsahují citlivá data musí být bezpečně likvidována, pokud již nejsou využívána.

Aby vždy byla dostupná potřebná kapacita pro zpracování a uchovávání dat, je nezbytné monitorovat kapacitní požadavky a plánovat budoucí požadavky.
"Bezpečné" operace AA musí být prováděny odděleně od normálních operací. AA odpovídá za následující bezpečnostní faktory: operační procedury a odpovědnosti, plánování ochran systému, ochrana před softwarovými útoky, vedení hospodaření, správa sítě, aktivní monitoring (auditní logy, události,...), práce s médii, výměna dat a softwaru.
Atributová autorita musí zajistit, že přístup do systému AA mají pouze oprávnění jedinci. Konkrétně:

- kontroly (např. firewall) musí být implementovány tak, aby chránili vnitřní síť AA před zásahy třetích stran z vnější sítě;
- citlivá dat musí být chráněna pokud jsou přenášena v nechráněné síti;
- AA musí zajistit efektivní administraci přístupu uživatelů (včetně operátorů, administrátorů resp. libovolného jiného uživatele, který má přístup do systému) tak, aby byla zajištěna bezpečnost systému a to včetně uživatelských účtů, auditů a dočasných modifikací či rušení přístupu;
- AA musí zajistit, že přístup k informacím a aplikacím je omezen podle politiky kontroly přístupu a že systém AA poskytuje dostatečné bezpečnostní kontroly pro oddělení důvěryhodných rolí. Zvlášť musí být kontrolovány systémové utility.

- personál AA musí být úspěšně identifikován a autentizován, dříve než začne používat kritické aplikace, které se vztahují ke správě atributových certifikátů. Jeho činnost je logována.
- citlivá data jsou chráněna před rozkrytím prostřednictvím nového použití dočasných úložišť, která jsou přístupna neoprávněným uživatelům (citlivými daty jsou i registrační údaje);
- AA zodpovídá za to, že komponenty lokální sítě (např. routery) jsou umístěny v zabezpečeném prostředí a jejich konfigurace je periodicky podrobována auditu.
- AA má vybavení pro neustálý monitoring a poplašný systém, který umožňuje detekovat, registrovat a včasně reagovat na libovolný neoprávněný přístup k jejím zdrojům;
- akviziční služba atributových certifikátů musí udržovat kontrolu pokusů subjektu získat atributový certifikát;
- obdobně musí být službou šíření kontrolovány přístupy, které mají za cíl přidat či odebrat atributový certifikát nebo modifikovat s nimi spojené informace;
- aplikace, která řídí odvolávání certifikátů musí udržovat kontrolu přístupu tak, aby bylo zabráněno neoprávněným pokusům aktivace či deaktivace funkcí atributových certifikátů;
- aplikace, která má na starosti statuty revokací musí udržovat kontrolu přístupu tak, aby byly kontrolovány pokusy o modifikaci revokačního statutu.

AA musí používat důvěryhodné systémy a produkty chráněné proti modifikacím. Musí být provedena analýza bezpečnostních požadavků v rámci libovolného projektu, který definuje systém AA tak, aby příslušné IT systémy obsahovaly potřebné bezpečnostní prvky. Pro případ změn (nové verze, modifikace, bezpečnostní záplaty softwaru) musí být definovány příslušné kontrolní procedury.

AA musí zajistit, že v případě neštěstí, živelné pohromy (včetně situací, kdy dojde ke kompromitaci podpisového klíče AA) bude činnost obnovena v nejkratší možné lhůtě.
Certifikát veřejného klíče patřícího ke kompromitovanému soukromému klíči musí být odvolán, tj. cesty pro ověření libovolného atributového certifikátu, který AA vydala a které se odkazují na zmíněný certifikát již déle neplatí.

AA musí zajistit, že v případě ukončení činnosti AA budou negativní dopady na klienty a spoléhající se strany minimalizovány. AA musí zajisti pokračování ošetření záznamů, které poskytují důkaz certifikace z legislativních důvodů.

AA musí zajistit shodu s požadavky, které má platná legislativa. Konkrétně:
- záznamy AA musí být ochraňovány tak, aby bylo zabráněno jejich ztrátě, zničení či falzifikaci. Některé údaje musí být uchovávány bezpečným způsobem.
- AA musí zajistit naplnění požadavků Evropské směrnice na ochranu dat (dle implementace v národních legislativách);
- musí být přijata vhodná technická a organizační opatření, která mají za cíl chránit před neautorizovaným či nezákonným zpracováním osobních údajů a před jejich ztrátou či poškozením;
- informace, které uživatelé předávají AA musí být chráněny před rozkrytím - pokud nedal uživatel souhlas nebo existuje soudní příkaz či jiný zákonný důvod.

AA musí zajistit zaznamenání všech relevantních informací, které se týkají atributového certifikátu a jejich uchování v potřebném časovém intervalu (např. z důkazního důvodu certifikace pro právní procedury).

AA musí zajistit svoji organizační spolehlivost. Konkrétně:

- politiky a procedury, kterými se AA řídí musí být nediskriminační;
- AA musí učinit své služby dostupné pro všechny žadatele, jejichž aktivity se shodují s deklarovanou oblastí působnosti AA;
- AA je právní entita ve smyslu národního zákona;
- AA má systém správy kvality a správy informační bezpečnosti, který odpovídá požadavkům poskytovaných certifikačních služeb;
- AA má uspořádání, které adekvátním způsobem pokrývá odpovědnosti, které plynou z jejích operací a aktivit;
- AA je finančně stabilní a má zdroje potřebné k činnostem dle své politiky;
- AA zaměstnává dostatečné množství personálu, který má odpovídající vzdělání, školení, technické znalosti a zkušenosti;
- AA má politiku a procedury pro řešení stížností a rozporů, které obdrží od zákazníků či jiných stran ve vztahu k poskytovaným elektronickým službám;
- AA má vhodným způsobem zdokumentovány smlouvy v místech, kde poskytování služeb se opírá o takovéto smluvní ujednání;

V závěru dokumentu je analyzován rámec pro jiné politiky pro AA (např. situace, kdy atributové certifikáty nejsou veřejně vydávány).

3. Závěr

Materiál obsahuje přílohy A-D. Přitom příloha A obsahuje požadavky na formát atributových certifikátů, příloha B se týká právních dopadů odpovědnosti AA dle dokumentů Evropské Unie.

Příloha C obsahuje poznámky k modelové prováděcí směrnici atributové autority, příloha D obsahuje bibliografické odkazy.

Celkově - rozsáhlý a obsažný materiál, s jehož hlavními částmi byl čtenář obeznámen ve čtyřech pokračováních, dává možnost poměrně podrobně nahlédnout do problematiky atributových autorit. Zatím možná otázkám vytváření vhodných přístupových modelů v počítačových sítích není věnována příslušná pozornost. Pokud se však chceme pohybovat v bezpečném a zároveň flexibilním počítačovém prostředí, nevyhneme se použití těchto či obdobných postupů.

4. Literatura

[1] Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates (ETSI TS 102 158, V.1.1), http://portal.etsi.org/esi/el-sign.asp
[2] rfc3281: An Internet Attribute Certificate Profile for Authorization
[3] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002

D. Použití zabezpečených serverů v síti Internet a prohlížeč Mozilla (pro začátečníky), část 1.

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

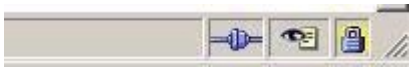
- **Úvod**
- **Modul Soukromí & Zabezpečení**
- **Správa certifikátů v Mozille**
- **Nastavení ověřování certifikátů v Mozille**
- **Nastavení SSL komunikace v Mozille**
- **Stažení certifikátu poskytovatele na disk**
- **Závěr**

Úvod

Pořídili jste si prohlížeč Mozilla a nevíte jak správně nastavit správu certifikátů a zajistit bezpečnou komunikaci se zabezpečenými servery? Pak tento krátký článek je určen právě vám.

Mnoho serverů v síti Internet je nastaveno tak, aby bylo neoprávněným osobám zabráněno získat informace odeslané z těchto serverů nebo na ně. Tyto servery se nazývají zabezpečené. Aplikace Mozilla podporuje protokoly zabezpečení používané zabezpečenými servery SSL 3.0, SSL 2.0, TLS 1.0.

Pokud navštívíte zabezpečený www server, odešle k vám výzvu na ustanovení zabezpečeného spojení a pokud dojde k dohodě, aplikace Mozilla zobrazí ve stavovém řádku ikonu zámku.



Nutnou podmínkou k ustanovení zabezpečeného spojení je :

- důvěra v certifikát (resp. v certifikační autoritu, která certifikát vystavila)
- samozřejmě časová platnost certifikátu
- správné umístění certifikátu na www stránce, pro kterou byl vydán

Z důvodu bezpečnosti takového spojení je dobré si uvědomit, že kontrola certifikátů se provádí proti seznamu zneplatněných certifikátů - Certificate revocation list (dále jen CRL), který je instalován na vašem PC, a proto je nutné nastavit pravidelné stahování těchto seznamů od společností, kterým důvěřujete (tj. které vydávají certifikáty na které se spoléháte).

Slovo „důvěra“ je v souvislosti s certifikáty často uváděno ve dvou, zcela odlišných významech. Oba pojmy se zaměňují, a proto se u nich krátce zastavíme.

První význam „důvěra“ v nějakého poskytovatele certifikačních služeb má technický aspekt. Znamená to, že kořenový certifikát tohoto poskytovatele je uložen v úložišti certifikátů vaší aplikace a důsledkem toho je, že „důvěřujete“ všem certifikátům, která tato společnost vydala – tj. při kontrole jsou označeny za ověřené a tedy důvěryhodné, pokud jsou současně splněny i další podmínky (např. doba platnosti certifikátu, certifikát není uveden na CRL atd.)

Druhý význam plyne z toho, jak sami s certifikáty vystavitelů (certifikačních autorit) zacházíte. Není jasné, proč se máte spoléhat na certifikáty poskytovatelů, které máte

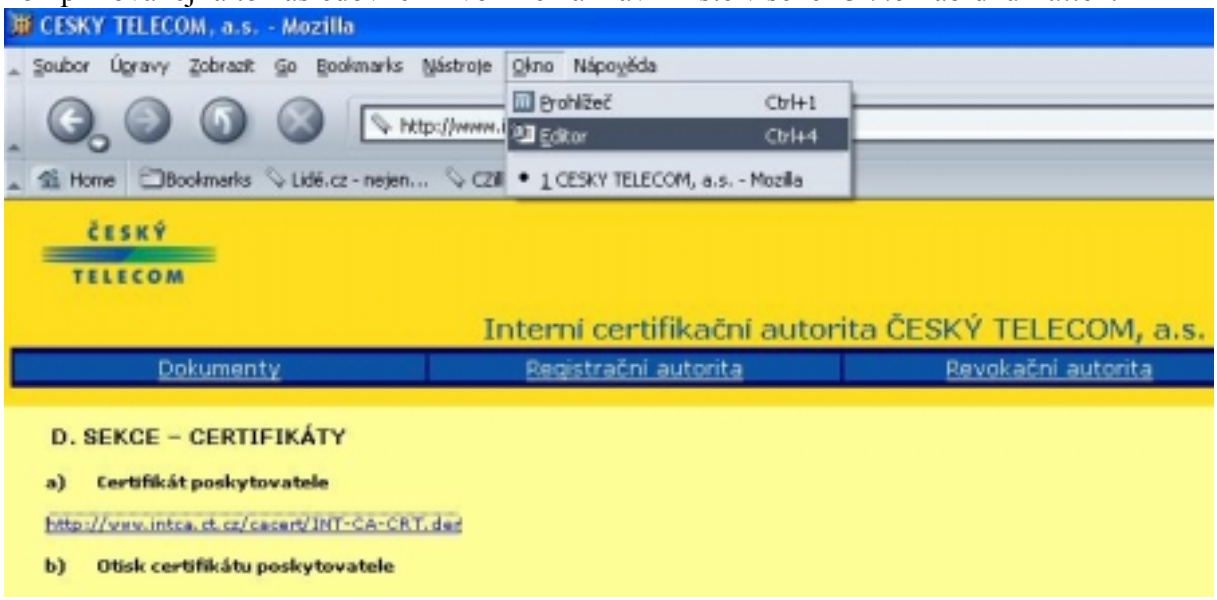
předinstalovány své certifikáty v úložišti certifikátů aplikace Mozilla, kterou jste si nainstalovali. Sami byste měli rozhodnout (zpravidla na základě Certifikační politiky, kterou daný poskytovatel vydává a podle níž vydává a vede správu certifikátů), zda vám způsob vydávání a správy certifikátů (včetně záruk za takto vydané certifikáty) vyhovuje. Při rozhodování je dobré vzít do úvahy zejména tato kritéria – zveřejnění certifikační politiky, její struktura a uvedené záruky za vydané certifikáty, způsob registrace vlastníka certifikátu, periodicita vydávání CRL, způsob žádosti o zneplatnění certifikátu, zveřejňování výsledků bezpečnostních auditů daného poskytovatele atd.

Měli byste tedy zvážit, které poskytovatele zde ponechat a které sem naopak přidat (např. v České republice by bylo vhodné zde mít certifikáty poskytovatelů, které vydávají koncovým uživatelům certifikáty podle zákona o elektronickém podpisu č.227/2000 Sb. (tzv. kvalifikované certifikáty) a certifikáty poskytovatelů na jejichž certifikáty se chcete výslovně spoléhat (např. certifikát banky se kterou komunikujete nebo certifikát interní certifikační autority firmy se kterou obchodujete nebo využíváte jejich služby atd.).

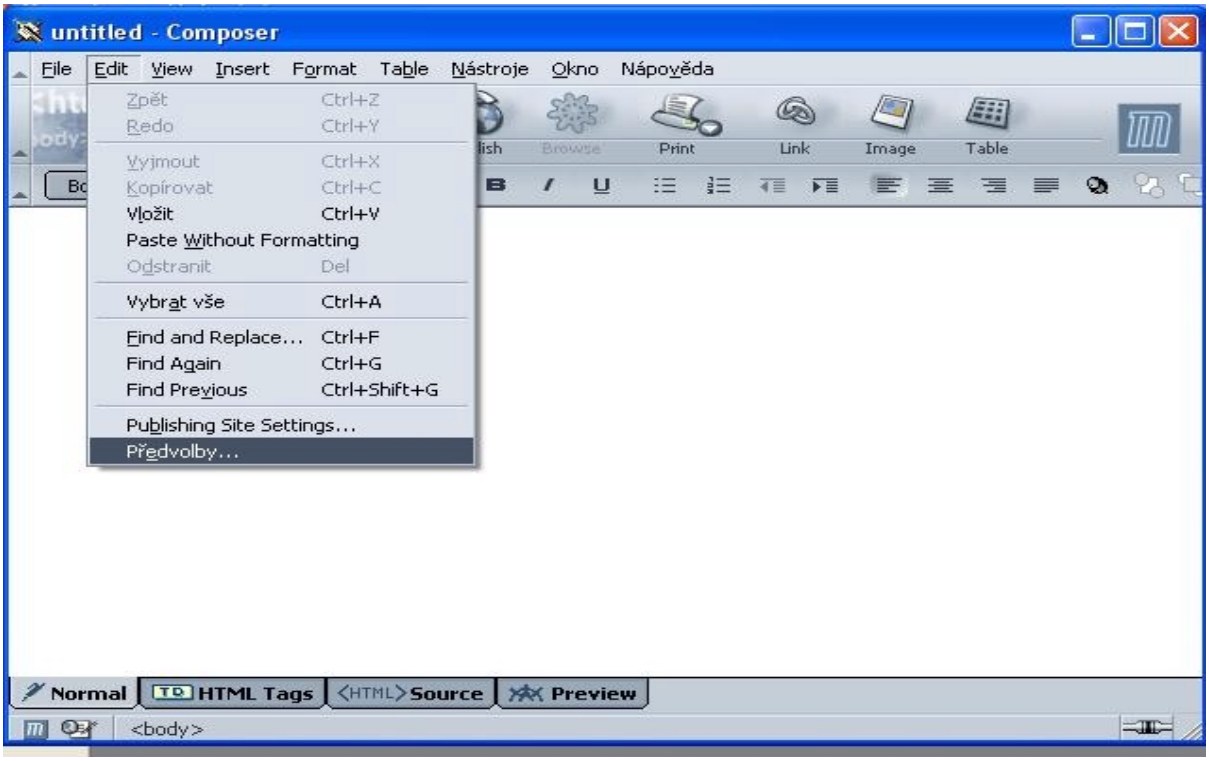
Modul Soukromí & Zabezpečení

Mozilla nepoužívá úložiště certifikátů, které spravuje MS Windows a které využívají aplikace přes Crypto-API (tj. Microsoft Internet Explorer, MS Outlook, atd.). V následujícím textu si proto ukážeme, jak lze úložiště certifikátů aplikace Mozilla spravovat a jak nastavit použití a pravidelné stahování CRL těch poskytovatelů na jejichž certifikáty se chceme spoléhat.

Certifikáty a CRL se spravují z modulu ke kterému se dostaneme poněkud komplikovaněji a to následovně – zvolíme na hlavní liště v sekci *Okno* nabídku *Editor*.

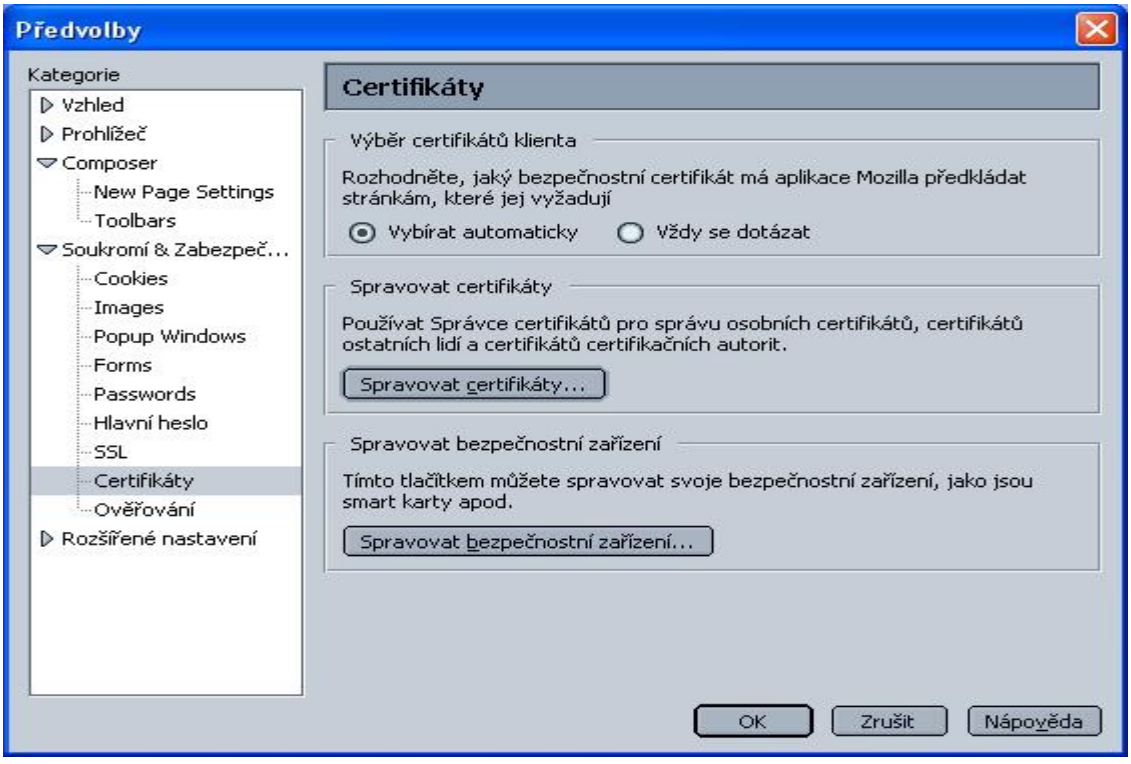


V novém okně se otevře modul Editor. V jeho horní liště volíme nabídku *Edit* a v roletovém menu, které se otevře vybereme *Předvolby*.

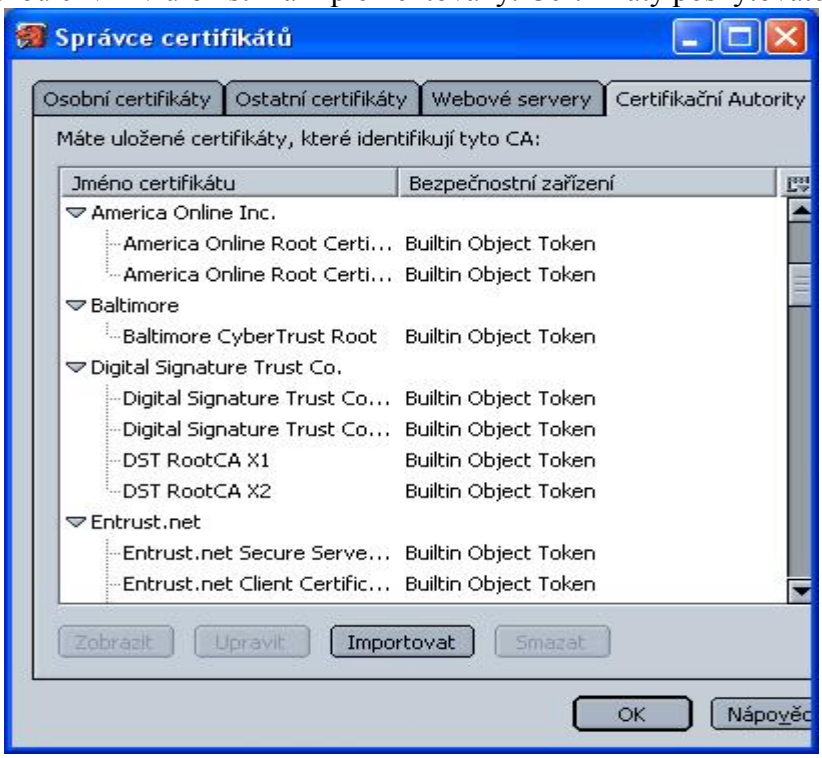


V levém sloupci se objeví položky, které lze v předvolbách nastavit. Pokud nejsou v levé části pod položkou *Soukromí & Zabezpečení* vidět žádné podkategorie, klikněte dvakrát na kategorii a rozbalí se vám seznam možností. Potom vyberte možnost *Certifikáty*.

Správa certifikátů v Mozille



Zvolte *Spravovat certifikáty* a zobrazí se okno ve kterém uvidíte seznamy certifikátů, které máte v danou chvíli v úložišti naimplementovány. Certifikáty poskytovatelů, kterým

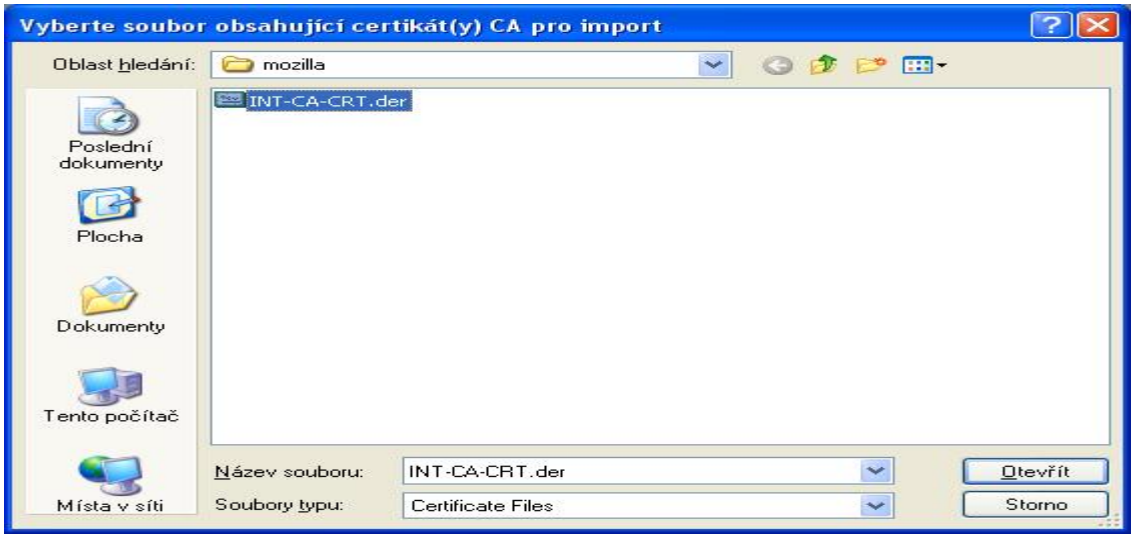


důvěřujete, naleznete v záložce *Certifikační Autority*.

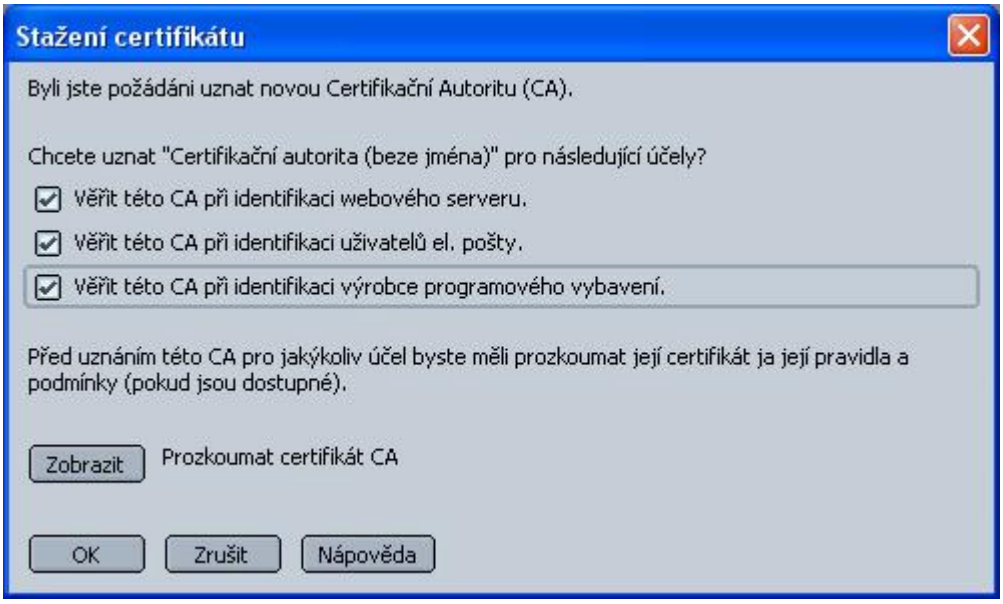
Pokud chcete certifikát některého z poskytovatelů z úložiště vyjmout, jednoduše jej vyberete (klikneme na něj myší) a následně v dolní části okna zvolte *Smazat*.

Vložit do úložiště certifikátů certifikát poskytovatele, kterému chcete důvěřovat, se děje opět velice jednoduše. Nejprve z důvěryhodného zdroje takovýto certifikát zkopírujte na plochu (nebo do nějakého adresáře). (Viz samostatná část stažení certifikátu poskytovatele na disk).

Následně ve *Správci certifikátů* zvolte *Importovat*. V okně, které se otevře vyhledejte na pevném disku certifikát poskytovatele, který chcete do kořenového úložiště uložit.

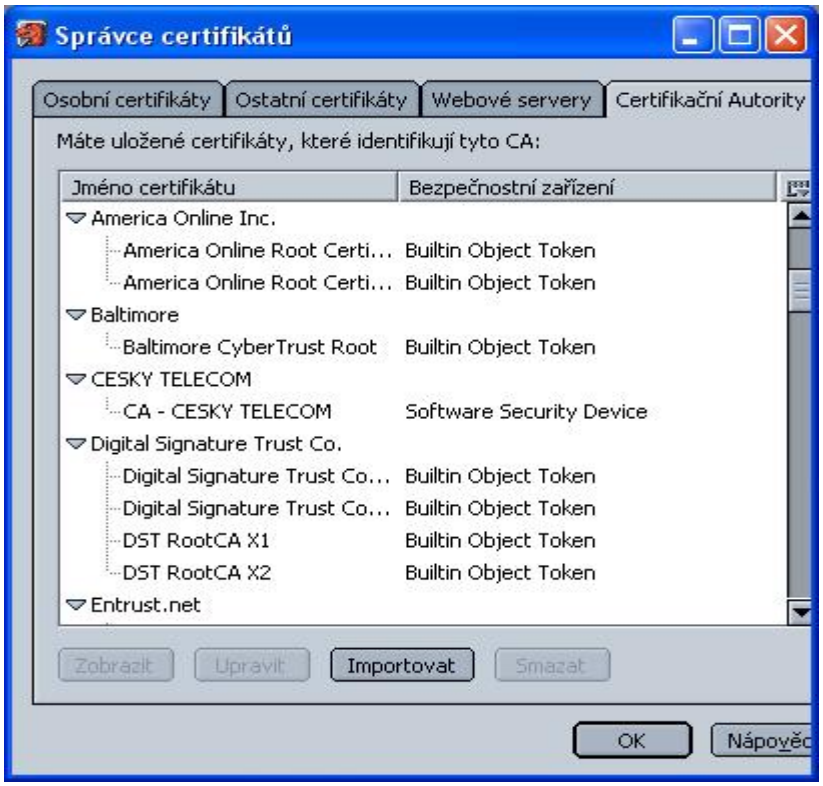


Otevře se okno „uznání certifikátu“ nového poskytovatele. Zde je potřeba vyplnit pro jaké účely má být certifikát poskytovatele považován za důvěryhodný.



Při volbě prvé možnosti budete věřit všem certifikátům, které vystavitel vydává pro identifikaci www serverů (pro identifikaci a SSL komunikaci).

Při druhé volbě budete věřit osobním certifikátům, které vystavitel vydává žadatelům o certifikáty určené pro šifrování a podepisování elektronické pošty a třetí možnost zajišťuje důvěru v certifikáty, které poskytovatel vydal pro podpis zdrojových kódů programů (updatů, bezpečnostních patchů atd.).



Po ukončení implementace lze nově instalovaný certifikát najít mezi již uloženými certifikáty ostatních poskytovatelů (v naší ukázce to je certifikát označený jako CA – CESKY TELECOM).

Ke bezpečnému ověření certifikátů, které tento poskytovatel vydává, zbývá nastavit použití CRL při ověření certifikátu a automatické stahování CRL.

E. Letem šifrovým světem

S některými vybranými událostmi v oblasti bezpečnosti IT a v kryptologii jste se mohli průběžně seznamovat v novinkách, které od začátku roku vedeme na domácí stránce našeho e-zinu (http://crypto-world.info/news/). Tyto novinky pro vás připravují Tomáš Rosa, Jaroslav Pinkava a Pavel Vondruška.

Podívejme se proto jen krátce, na přehled důležitých standardů a norem z oblasti PKI, které byly v tomto období publikovány.

1) **Návrh novely zákona o elektronickém podpisu** ve třetím čtení schválila Poslanecká sněmovna (31.3.2004). Zákon nově umožňuje používání takzvaných elektronických značek, kterými mohou být označovány datové zprávy, a kvalifikovaných časových razítek. Zákon ještě musí schválit Senát a podepsat prezident republiky.
http://technet.idnes.cz/zprava.html?zprava=27717

2) Některé publikované standardy v rámci EESSI Program - **ETSI Electronic Signatures and Infrastructures**
XML Advanced Electronic Signatures (XAdES), TC ESI, TS 101 903 v1.2.2,
http://portal.etsi.org/esi/el-sign.asp#TS%20101%20903

X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, ETSI, TS 102 280
http://portal.etsi.org/esi/el-sign.asp#TS%20102%20280

Qualified Certificate Profile, ESI, TS 101 862 v.1.3.1
http://portal.etsi.org/esi/el-sign.asp#TS%20101%20862

3) **National Institute of Standards and Technology** – USA – vydal velmi zajímavé publikace:

Final Draft Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
http://csrc.ncsl.nist.gov/publications/drafts/SP800-37-finaldraft.pdf

NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
http://csrc.ncsl.nist.gov/publications/drafts.html#sp80060

4) **RFC** :
RFC 3739 on Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
ftp://ftp.rfc-editor.org/in-notes/rfc3739.txt

Pro ty, kteří mají rádi aprílová čtení – můžeme posloužit i jedním speciálním RFC.
Nejedná se samozřejmě o vážně míněný dokument RFC, ale o dílko, které vtipným způsobem (obsahem i zpracováním) je parodií na skutečná RFC.
RFC 3751 Omniscience Protocol Requirements. S. Bradner. 1 April 2004.
(Format: TXT=20771 bytes) (Status: INFORMATIONAL)
ftp://ftp.rfc-editor.org/in-notes/rfc3751.txt

O čem jsme psali v dubnu 2000 - 2003

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

Crypto-World 4/2003

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 21 dní po jeho rozeslání) a předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@ct.cz