Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 5/2004 **17. květen 2004**

5/2004

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Začněte používat elektronický podpis
Ing. Petr Komárek, CA Czechia, s.r.o.

Většina čtenářů Crypto-Worldu pravděpodobně již zná základy elektronického podpisu, umí si nastavovat své poštovní klienty, zálohovat certifikáty a také alespoň částečně zná principy fungování elektronického podpisu. Pokud však ještě nemáte s elektronickým podpisem (dále jen EP) žádné zkušenosti, víte co byste měli udělat ještě před tím, než jej začnete používat?

Naše zkušenosti jsme shrnuli do tří základních bodů, které by měl začínající uživatel udělat předtím než EP začne používat:

1/ **Seznámit se** se základními **principy a pravidly** činnosti a používání EP. Většina certifikačních autorit na svých stránkách takovéto popisy má a také na internetu a v tisku se dá najít dost zajímavých článků o EP. Není nutné vědět co to je RSA, DSA, MD5. Avšak to, že existuje CRL (Seznam zneplatněných certifikátů), který je nutný kontrolovat, nebo že existují jakési dva klíče ze kterých ten soukromý se nesmí nepovolané osobě dostat do rukou, by rozhodně bylo dobré vědět.

2/ **Zvolit si certifikační autoritu**. Pokud bude chtít uživatel používat podpis pro komunikaci se státní správou, jeho rozhodnutí je velice „jednoduché“, jelikož si musí zvolit akreditovanou certifikační autoritu a tou je v ČR zatím jediná a to I.CA. Pokud chce EP používat ke komunikaci s partnery, přáteli, podepisovat data nebo komunikaci šifrovat, má již širší výběr. Je možné se orientovat dle ceny, Certifikační politiky, frekvence aktualizací CRL a hlavně podle důvěryhodnosti. Není totiž problém zdarma a hned na internetu získat certifikát, ale pokud je vystaven bez jakéhokoliv ověření, pro příjemce nemusí být takto podepsané zprávy důvěryhodné a komunikace založená na takovýchto certifikátech akceptovatelná.

3/ **Otázka kompatibility**. V okamžiku, kdy si certifikační autoritu vyberete, doporučujeme otestovat funkčnost elektronického podpisu a vámi používaného systému. Proto certifikační autority nabízejí testovací certifikáty s omezenou platností (15 dní až 1 měsíc).

Jakmile uživatel úspěšně projde těmito třemi body, nic mu nestojí v cestě, aby si zažádal o certifikát k elektronickému podpisu u certifikační autority, kterou si vybral.

Certifikační autorita Czechia (www.caczechia.cz) vytvořila na svých stránkách jednoduché průvodce, které zájemce provedou v několika přehledných krocích celým procesem žádosti o certifikát.

Plnohodnotný osobní certifikát zdarma

A na závěr pro vás máme malé překvapení. Čtenáři e-zinu Crypto-World mohou ZDARMA získat plnohodnotný osobní certifikát od Certifikační autority Czechia a to na základě zadání tohoto kódu:

NMDR-1AAV-RAR8

Kód je platný do konce května 2004 *a není omezen počtem objednaných certifikátů !*

B. Program STORK - vstupní dokumenty, příprava E-CRYPT
Jaroslav Pinkava, PVT a.s.

1. Úvod

O iniciativě Cryptonessie byli čtenáři Crypto-Worldu informování nejednou. Práce zde však v zásadě skončili (pokračuje se přípravou konkrétních norem). V dubnových novinkách Crypto-Worldu proběhla (mimo jiné) informace o navazující evropské iniciativě v kryptografické problematice **E-CRYPT**.

Na webovských stránkách (http://www.stork.eu.org/documents.html) nalezneme odkaz, že tato iniciativa vznikla na základě priorit výzkumu a vývoje stanovených v dokumentu [1] . V tomto materiálu je definovaná množina strategických cílů (výzkumu a vývoje) a jedním z nich (*Towards a global dependability and security framework*) jsou formulovány požadavky směrem k bezpečnosti informací, komunikačních systémů a infrastruktur. Konkretizací tohoto cíle směrem ke kryptologii je požadavek na vývoj, testování a verifikace současných a nových kryptografických technologií pro široké spektrum aplikací. Materiál [1] však zatím neobsahuje požadavky směrem k dalšímu rozvoji kryptografické teorie. V rámci ročního projektu **STORK** (začal v červenci roku 2003), který byl součástí pátého rámcového programu byly zpracovány vstupní dokumenty.. Předpokládám, že po ukončení projektu budou zveřejněny jeho výsledky. Projekt STORK slouží jako startovní plocha projektu E-CRYPT. Samotný projekt E-CRYPT byl zahájen 1.února 2004.

Zveřejněné tři výchozí dokumenty si zasluhují pozornost kryptografické veřejnosti. Jsou to:

1. New trends in Cryptology
2. Research agenda for the Future of Cryptology
3. Open Problems in Cryptology,

publikovány byly v květnu a červnu 2003 (viz lit. [2], [3], [4]). Zatím je známo, že projekt je rozdělen na čtyři části, jedna z nich je věnována symetrické kryptografii. Prvotními cíly této části jsou - vývoj nové rychlé proudové šifry a také další hodnocení normy AES (viz [6]).

Dalším zajímavým zveřejněným dokumentem je materiál [5], který obsahuje přehled významných evropských kryptologických pracovišť. Jedná se o firmy pracující v tomto oboru (Česká republika zde nemá žádného zástupce) a také o akademické kryptologické týmy (zde z České republiky najdeme jména J.Hrubý - ČSAV a V.Matyáš + J.Staudek - MU Brno; ze Slovenska je zde O.Grošek - FEI STU).

Každý ze tří výše zmíněných dokumentů (pro jednoduchost dalších odkazů, které budou časté, je označíme – v té posloupnosti, jak jsou výše uvedeny - jako materiály **M1, M2, M3**) má obdobnou strukturu:

1. Úvodní kapitola
2. Kryptografie v informační společnosti
3. Kryptografické protokoly
4. Kryptografické techniky
5. Matematické základy

Tento článek (a jeho pokračování – druhá část) budeme strukturován obdobně. Nejprve se tedy budeme zabývat problematikou kryptografie v informační společnosti a to z hlediska všech tří dokumentů, pak obdobným způsobem kryptografickými protokoly. V druhé

části článku bude popsána problematika kryptografických technik a problematika matematických základů kryptografie.

Poznámka: Samozřejmě zájemcům o hlubší seznámení se s problematikou doporučujeme prostudovat si materiály samotné.

2. Kryptografie v informační společnosti

Materiál M1 je členěn v této kapitole následovně:

2.1 Bezpečná komunikace
2.2 Finanční služby
2.3 Sociální aspekty

K bodu 2.1: Nově v oblasti bezpečné komunikace nastupují technologie vyžadující zabývat se *bezpečností mobilních systémů*. Nevede to k vzniku potřeby nových zásadních výsledků na poli kryptografie, jsou to spíše aplikace teorie již existující. Některé aspekty mobilních telefonů však mají svá specifika. Např. je vhodnější používat proudové šifrování, algoritmy musí umožňovat implementace málo energeticky náročné, musí být spustitelné na SIM kartách (a čipových kartách vůbec), i majitel takové karty se nesmí dostat ke kryptografickým klíčům (či dokonce k některým postupům šifrovacích algoritmů). Implementace musí vylučovat možné útoky z postranních kanálů, jsou pro potřeby bezpečných sítí mobilní telefonie vyvinuty speciální protokoly, speciální kryptografické algoritmy (KASUMI), mobilní telefony jsou kombinovány z dalšími službami (el.platby, autentizace,...).

Bezpečnost sítí je jednou z nejdůležitějších aplikací kryptografie. Hlavními problémy bezpečnosti zde jsou:
- zajistit, aby neoprávněná strana nemohla provádět průniky či modifikovat provoz sítě;
- chránit síť jak z hlediska logického tak fyzického před vnějškem (pomocí specifického HW a SW jako firewally, systémy detekce průniků atd.).

Kryptografie se zabývá prvním z těchto dvou bodů, pro potřebné separace aktérů v síti byla vyvinuta celá řada bezpečnostních protokolů a modelů klíčového hospodářství (např. IPSEC, IKE). V posledních létech je v těchto souvislostech intenzivně studována také prokazatelná bezpečnost.

K bodu 2.2: *Elektronické platby* dnes vystupují v celé řadě heterogenních podob (digitální peněženky, elektronický peněžní styk, mikroplatby,...). Je používána celá řada protokolů na bázi symetrické i asymetrické kryptografie. Z hlediska kryptografických aplikací je atraktivní výzkumnou oblastí digitální (elektronický) peněžní styk. Anonymní elektronické platby reprezentují výzkumy Davida Chauma. Zajímavou problematikou jsou *slepé podpisy* (blind signatures), studovány jsou také v návaznosti na *prokazatelnou bezpečnost*. Je zde vytvářena celá řada konkrétních modelů s různorodými vlastnostmi.

K bodu 2.3: Dopady popisovaných technologií na podobu společnosti jsou nezpochybnitelné a objevují se v celé řadě často i nečekaných souvislostí. Potenciál počítačových technologií se včleňuje do široké škály praktických aplikací velice různých typů – včetně miniaturizovaných zařízení, bezdrátových sítí, principy robotiky a automatizovaných výrob jsou využívány stále šířeji atd. Bezpečnostní požadavky zde vznikající mají i některé nové vlastnosti – např. díky miniaturizaci musíme pracovat s omezenými zdroji (CPU, RAM), je nezbytné hledat ochrany

proti útokům, které mají za cíl zamezit využití určité služby, nároky na používané klíčové hospodářství v sítích typu ad-hoc jsou komplikovanější atd.

Pojem *časové značky* – umožňuje nám stanovit, že určitý digitální objekt byl vytvořen či podepsán před daným časovým okamžikem – v návaznosti na služby autority časových značek TSA dává důležitý prostředek nezbytný pro podchycení celé řady vznikajících bezpečnostních nároků. Příkladem může být elektronický obchod, podpis elektronických smluv, EDI, multimediální služby atd. Časové značky slouží také jako nezbytný prostředek, který podporuje nepopiratelnost elektronických podpisů. V návaznosti na aparát časových značek jsou využívána také tzv. linkovací schémata (zajišťují provázanost vytvářených časových značek a tím pádem vedou k větší bezpečnosti poskytovaných služeb časových značek) a tzv. distribuční schémata (součinnost více TSA, více uživatelů).

Elektronické hlasování - v materiálu jsou popsány čtyři základní používaná schémata, žádné z nich ale není považováno za ideální – je oblast, kde byť odpovídající teorie je bohatá, není však uspokojující.

Správa digitálních práv (Digital Rights Management – DRM) je další širokou oblastí, která se často opírá o využití kryptografických metod. Jedná se především o problematiku ochrany autorských práv (pro díla v digitální podobě). Cílem DRM je, aby digitální obsah byl přístupný pouze pro oprávněné uživatele. Existuje celá řada používaných technik (kryptografické primitivy a protokoly, vodoznaky, otisky, specifický HW, specifické modely klíčového hospodářství).

Materiál M2 je členěn v této kapitole následovně:

2.1 Bezpečná komunikace
2.2 Digitální peněženky, elektronický platební styk a mikroplatby
2.3 Sociální aspekty

K bodu 2.1: *Současné preference výzkumu jsou v rámci mobilních systémů* směrovány na vývoj algoritmů a jejich implementací s minimálními nároky na spotřebu proudu. Jsou také řešeny otázky, které jsou spojeny především s ekonomickými nároky projektů (spíše než s technologickými), nedaří se ještě stále vhodně propojit otázky bezpečnostní a ekonomické takovým způsobem, aby výsledek byl v praxi dlouhodobě využitelný.

Z hlediska *bezpečnosti sítí* je dnes ještě stále mnoho otázek, které souvisí s bezpečnostní analýzou používaných protokolů, důkazů jejich bezpečnosti atd. Některé používané protokoly by měly být nahrazeny tak, aby např. robustněji odolávaly útokům, které mají za cíl zamezit poskytnutí požadované služby (DoS attack – Denial of Service attack). Také rostoucí množství ukládaných, přenášených a zpracovávaných dat vede k novým rizikům a novým potřebám z hlediska používaných kryptografických transformací (gigabajty šifrování a dešifrování).

K bodu 2.2: Bezpečnost většiny schémat pro spravedlivý *elektronický platební styk* v literatuře se opírá o schéma, které navrhl Brands (restrictive blind signature scheme). Teorie však zatím stále nedodala v tomto směru potřebné důkazy o bezpečnosti daného schématu (za standardních předpokladů – složitost diskrétního logaritmu nebo složitost Diffie-Hellmanova postulátu). Nevýhodou off-line schémat je jejich nepraktičnost.
K bodu 2.3: Zde je nejprve zmíněna celá řada norem, které vznikly či vznikají v rámci EESSI – v návaznosti na Směrnici EU o elektronickém podpisu (ETSI, CEN/ISSS). *Časové značky* jsou ne tak dávným "vynálezem" a technologie, které se o ně opírají nejsou často ještě

dostatečně zralé. Objevuje se např. pojem intervalových časových značek, které poskytují vyšší stupeň důvěry (ve vztahu k potenciální nepřátelské TSA).

Používaná schémata pro *elektronické hlasování* jsou bohužel buď nedostatečně efektivní, nebo se opírají o nerealistické předpoklady.Hlavním úkolem zde je tedy návrh praktického a bezpečného schématu pro elektronické hlasování.

Správa digitálních práv je zatím relativně mladou problematikou a dokonce stále ještě existují pochyby o tom, zda je možné najít modely, které poskytují plnou ochranu digitálního obsahu.

Málo je známo o teorii pro software, který by byl odolný proti narušením (tamper resistant software). Nové technologie opírající se o použití digitálních vodoznaků se opírají o použití kryptografických technik se specifickými nároky. Vzniká však otázka praktičnosti existujících modelů, tj. jsou zde potřeby nových pohledů. Důležitým konceptem vyvinutým pro DRM je schéma BE (Broadcast Encryption), je zde však ještě celá řada otázek, které je nutno dále rozpracovat (množství klíčů, dlouhodobé BE schéma, procesy odvolání klíčů atd.).

Materiál M3 je členěn v této kapitole následovně:

2.1 Bezpečnost sítí a mobilních sytémů
2.2 Digitální peněženky, elektronický platební styk a mikroplatby
2.3 Inteligence okolí (prostředí)
2.4 Časové značky
2.5 Elektronické hlasování
2.6 Správa digitálních práv

V bodě 2.1 jsou jako otevřené problémy pro výzkum formulovány potřeby analýzy existujících bezpečnostních protokolů a protokolů pro distribuci klíčů (IPSEC, IKE, TLS,...), které by poskytly formální důkazy bezpečnosti (ve zdůvodněných modelech útoků protivníka). Je hledáno bezpečné efektivní schéma proudové šifry. Výzkumu otevřenou je také problematika optimalizace protokolů (složitostní hledisko a hledisko počtu relací).

Pro bod 2.2 jsou formulovány následující potřeby výzkumu:
- prokazatelně bezpečné platební schéma;
- nové elektronické platební schéma umožňující revokaci anonymity
- zvýšit efektivitu existujících schémat
- zkoumat alternativní cesty pro konstrukci digitálních platebních schémat.

V bodě 2.3 se jedná především o kryptografii, která je minimálně náročná na zdroje (paměť, spotřeba proudu, HW, malé hodnoty parametrů kryptografického schématu atd.).
Pro problematiku časových značek v bodě 2.4 jsou doporučovány např. následující výzkumné problémy :
- pokud dojde k rozbití použité hashovací funkce, měla by být k dispozici technika, která pomůže situaci vyřešit;
- najít praktické distribuované schéma vytváření časových značek.

V současné době elektronické hlasování(bod 2.5) v podstatě nepředstavuje žádnou výhodu oproti klasickým postupům. Hlavním cílem je zde tedy definovat praktické schéma.
Jak již bylo zmíněno výše, zásadním teoretickým problémem DRM (bod 2.6)je určit, zda je v principu možné konstruovat DRM systém, který může kompletně chránit digitální obsah (v zdůvodněném bezpečnostním modelu). Je zde také řada úkolů, které se týkají konkrétních problematik (HW+SW, vodoznaky, BE).

3. Kryptografické protokoly

Protokoly pro dvě komunikující strany lze rozdělit (**materiál M1**) na protokoly pro on-line autentizaci, autentizaci off-line a problematiku bezpečného komunikačního kanálu.
Autentizace (on-line) se v informační společnosti opírá o předpoklad, že dokazující strana má ve svém držení určitá specifická utajovaná data a veškerá komunikace probíhá pouze digitálně. Jsou zde nezbytné následující tři komponenty:

- možnost generování těchto utajovaných digitálních dat;
- tato digitální dat mohou být provázána s jinými digitálními daty, které má k dispozici ověřující strana;
- tato digitální dat slouží pak jako důkaz, který přesvědčí ověřující stranu, že dokazující strana má ve svém držení příslušné tajemství.

První komponenta je často realizována různými osobními zařízeními (čipové karty,...), biometrikou, někdy heslem atd. Druhá komponenta se odvíjí od použitého modelu správy klíčů a infrastruktury veřejných klíčů, třetí je pak hlavní kryptografickou komponentou – obvykle se nazývá identifikačním protokolem. Současné modely identifikačních protokolů se velice často opírají o různé typy důkazů (prokazatelná bezpečnost).

Off-line autentizace vychází z obdobných principů, liší se samozřejmě podobou interakce obu stran. Využívány jsou nejvíce dvě základní techniky – MAC (message authentication code) a digitální podpisy.

Problematika ustavení *bezpečného komunikačního kanálu* je jedním z nejstarších problémů kryptografie. Obvykle sestává ze dvou fází. V prvé se komunikující strany dohodnou na technice, která bude použita k šifrování/dešifrování. Potom jedna strana zasílá druhé zašifrovaná data, která může dešifrovat pouze tato druhá strana. Obvykle to proběhne takto –strany se dohodnou na použitém symetrickém šifrovacím algoritmu a na příslušném tajném klíči. Tajný klíč je přenesen buď jiným bezpečným kanálem, nebo jsou použity techniky asymetrické kryptografie. Všechny související používané protokoly se musí opírat o vhodný prostředek autenizace.

Protokoly pro více komunikujících stran (multiparty protocols) se týkají některých specifických oblastí jako jsou např. souběžné výpočty (kterých cílem může být např. dohoda na společném kryptografickém klíči či společném tajemství). Z hlediska formálních modelů bezpečnosti jsou v této souvislosti studovány vlastnosti kryptografických protokolů v kontextu jejich "samorozložitelnosti" (self composability), kdy běží souběžně více provedení téhož protokolu. Neplatí totiž obecně, že bezpečnost individuálního běhu protokolu implikuje bezpečnost simultánních průběhů.

V *problematice klíčového hospodářství a ustavení klíčů* existuje dnes ISO norma (ISO/IEC 11770 § Information technology – Security techniques – Key Management, Part1 - Framework, Part 2 – Mechanisms using symmetric techniques, Part 3 - Mechanisms using asymmetric techniques), ve které je definována široká škála protokolů. Běží také práce na projektu NIST, který se touto tématikou zabývá (poznámka autora – viz také Crypto-World 2003/02).

Infrastruktura veřejných klíčů (PKI) - v této problematice dnešní výzkum se týká zejména následujících okruhů problémů:

- modely důvěry (různých typů – hierarchické, síť důvěry (PGP – web of trust), a dalších);
- rozkrytí cesty (path discovery) pro automatické ustavení vztahu důvěry;
- jsou studovány alternativní modely jako SPKI, SDSI;
- efektivní cesty pro revokaci.

Narůstající množství dat, která jsou dnes ukládána a zpracovávána elektronicky se stává i určitou hrozbou z hlediska soukromá jednotlivých uživatelů. Kryptografie zde může sloužit jako technika, který poskytuje prostředky pro *utajení* resp. *anonymitu* uživatelů. V těchto souvislostech je zkoumána celá řada konkrétních technik, které jsou nebo mohou být za tímto účelem využívány.

Protokoly opírající se o využití kvantové kryptografie byly dnes již realizovány celou řadou institucí (včetně komerčních realizací). Bezpečnost těchto metod je stále zkoumána, v ideálním modelu platí sice obecný důkaz bezpečnosti (vyplývající z principu této technologie), avšak konkrétní implementace umožňují celou řadu dalších potenciálních útoků.

Materiál M2 v části, která se týká *protokolů pro dvě komunikující strany* se zmiňuje o potřebě výzkumu v následujících okruzích. Při generování tajemství – často zařízení, kterému je tajemství svěřeno není pro tyto účely vhodné. Zmiňovány jsou techniky pro vytváření zapamatovatelných tajemství s dostatečnou entropií (z hlediska jejich bezpečnosti). Dnešní identifikační protokoly se opírají o použití MAC či digitálních podpisů, autoři doporučují zkoumat techniky, které by byly vyvinuty speciálně pro tento účel. Bezpečnost některých protokolů stále ještě není dostatečným způsobem zanalyzována (three-pass protocols).
V problematice off-line autentizace je doporučováno hledat cesty jak používaná schémata (MAC a digitální podpisy) realizovat rychlejší, ale i bezpečnější cestou.

Protokoly pro více komunikujících stran – zde je doporučováno hledat další vazby s protokoly pro dvě komunikující strany a to tak, aby byla umožněna potřebná (z hlediska bezpečnosti) formální analýza těchto protokolů. Při studiu formálních bezpečnostních modelů se objevuje nový pojem univerzální rozložitelnosti (universal composability), který svým způsobem garantuje bezpečnost aplikace i při jejím běhu v změněných podmínkách. Některé dnešní formální bezpečnostní modely jsou však příliš restriktivní (a v tomto směru málo ohebné, tj. protokoly přestávají být v nastalých změnách bezpečnými). Je třeba hledat více adaptivní bezpečnostní modely. Důležitým trendem kryptografického výzkumu je zvažování útoků, které používají *kvantové technologie*.

V problematice *klíčového hospodářství* je zmíněna potřeba dalších výzkumů, které se budou týkat kryptografie opřené o ID (mohla by být touto cestou vyřešena řada problémů klíčového hospodářství. Pro PKI stále je otevřeným problémem otázka jak organizovat samo PKI. Existuje řada modelů – je potřeba je hlouběji zanalyzovat a přijít popřípadě i s novými návrhy. Problém revokace klíče je v této souvislosti jednou z centrálních otázek.
Podpisová schémata, která poskytují utajení (slepé podpisy a skupinové podpisy) jsou problematikou, na kterou ukazují autoři z hlediska potřeb výzkumu, který se týká technik pro *utajení*. Úplná *anonymita* je často zneužívána, měla by být proto v některých aplikacích pouze podmíněnou. Dnes toto umožňuje pouze málo šifrovacích schémat.

Protokoly kvantové kryptografie – nejznámějším dnes je kvantová výměna klíčů. Řada detailů konkrétních implementací stále vyžaduje pozornost analytiků a potřebu doplnit příslušné důkazy bezpečnosti. Kvantové protokoly jiných typů (než kvantová výměna klíčů) jsou také důležitým trendem výzkumu. Samotný kvantový kanál vyžaduje fundamentálnější pohled z hlediska jeho kryptografických vlastností.

Otevřené výzkumné problémy v oblasti kryptografických protokolů definuje **materiál M3** následovně. Pro *protokoly pro dvě komunikující strany* jsou jmenovány následující:

- prozkoumat bezpečnost složených autentizačních protokolů a protokolů pro dohodu na klíči, které sestávají z posloupnosti různých autentizačních protokolů (v rámci analýzy pojmu tzv.univerzálně rozložitelné bezpečnosti).

- vyvinout praktický a robustní rámec pro kombinaci dvou různých protokolů tak, aby vznikl jeden silný protokol (autentizační či protokol o dohodě na klíči).

Pokud se týká autentizace (on-line ~ identifikace+ resp. off-line ~ autentizace dokumentu), pak je zde nejprve poukázáno na problematiku schémat s nulovou znalostí (zero-knowledge), Jiným zde důležitým okruhem je koncepce skupinové identifikace (uživatel se identifikuje jako člen určité skupiny a přitom nerozkryje svoji identitu). Následně je formulována celá řada dílčích problémů (distribuce veřejných dat – např. pro verifikaci hesla; adaptace MAC a podpisů pro protokoly typu výzva-odpověď;, verifikace serverem v protokolu s nulovou znalostí; přesné stanovení bezpečností tří průchodových protokolů atd.).

V případě *protokolů pro více komunikujících stran* jsou vytyčeny mj. následující úkoly:
- najít efektivní (a dokonce praktický) protokol pro provádění operací s kryptosystémem s tajným klíčem sdílenou cestou (dnes jsou používány takto výlučně kryptosystémy s veřejným klíčem);
- nalézt praktický protokol pro bezpečné výpočetní aplikace mezi dvěma stranami;
- prozkoumat protokoly, které pracují se spolupracujícími stranami a zjednodušit jejich nároky na komunikaci;
- prozkoumat bezpečnost celé řady dalších protokolů, resp. navrhnout jejich bezpečnější modifikace.

V analýze formálních modelů bezpečnosti je např. formulován úkol definovat formální model popisující situace, kdy útočník má k dispozici kvantový potenciál.

V problematice *klíčového hospodářství* je zmíněn následující zajímavý problém. V kryptosystému, který navrhli Boneh a Franklin (ID-based) a který používá Weilovo zpárování na supereliptické křivce, najít multilineární zobecnění Weil/Tateova zpárování, které by bylo z výpočetního hlediska dostatečně efektivní. V současné době existují schémata pro dohodu na klíči pouze pro dvě či tři strany. Je třeba najít zobecnění pro více stran.

Schémata pro *utajení* – zde důkazy bezpečnosti všech používaných protokolů jsou prováděny použitím modelu náhodného oráklu, schémata, kde je dokázána "skutečná" bezpečnost jsou zajímavá pouze teoreticky. Bylo by užitečné nalézt praktické schéma slepého podpisu, které je prokazatelně bezpečné i mimo model náhodného oráklu.

Také pro kvantové kryptografické protokoly je formulováno několik úkolů – např. jsou požadovány důkazy bezpečnosti pro konkrétní návrhy protokolů či prototypů. Nebo – najít nové aplikace pro kvantovou kryptografii.

Poznámka: V druhé polovině článku budou zmíněny dva zbývající okruhy: kryptografické techniky a matematické základy.

Literatura

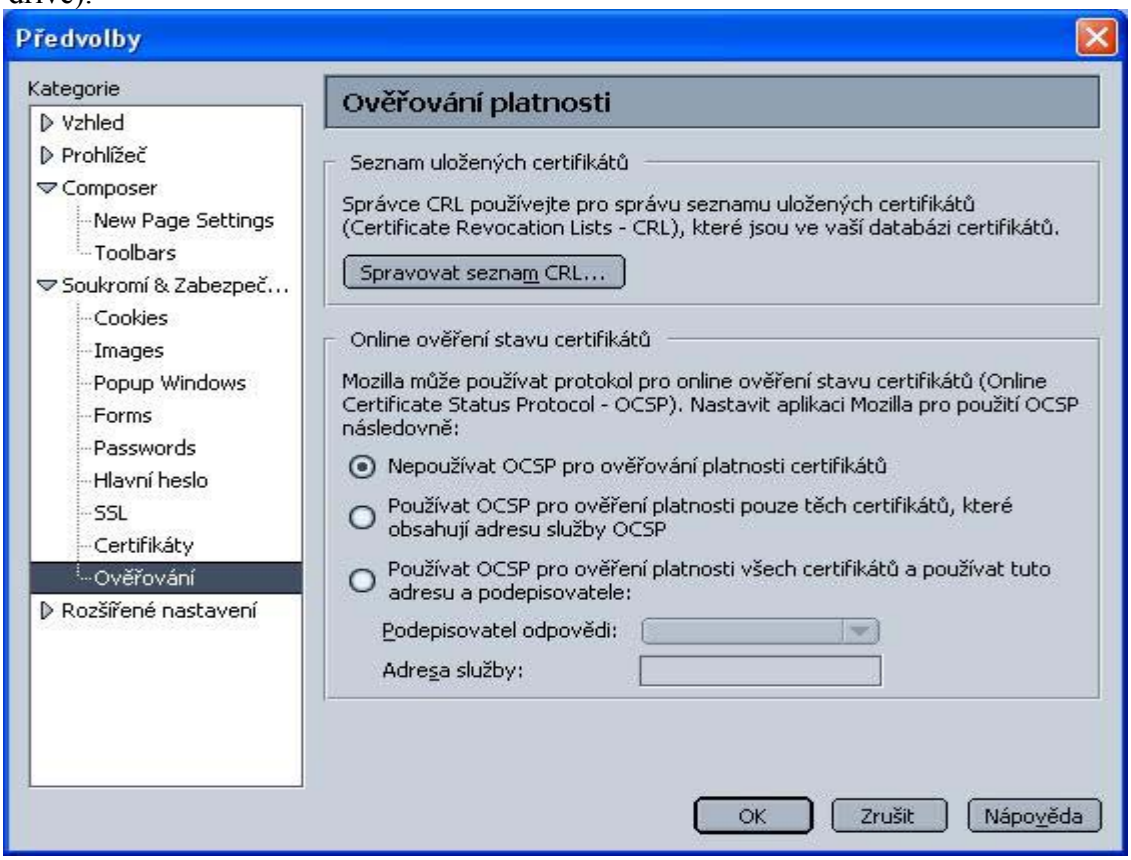
[1] Information Society Technologies, 2003-2004 Workprogramme, http://www.stork.eu.org/FP6/SP1-Priority-2-ist.doc
[2] http://www.stork.eu.org/documents/ENS-D4-1_4.pdf
[3] http://www.stork.eu.org/documents/RUB-D5-2_1.pdf
[4] http://www.stork.eu.org/documents/RUB-D6-2_1.pdf
[5] http://www.stork.eu.org/documents/KUL-D2_3-1_11.pdf
[6] Birjukov, Alex: Block Ciphers and Stream Ciphers: The State of the Art, http://eprint.iacr.org/2004/094.pdf

C. Použití zabezpečených serverů v síti Internet – Mozilla (pro začátečníky) část 2.

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

Nastavení ověřování certifikátů v Mozille

Parametry ověřování certifikátů vydaných poskytovateli certifikačních služeb se nastavují v modulu *Soukromí & Zabezpečení* v kategorii *Ověřování* (přístup k tomuto modulu viz dříve).



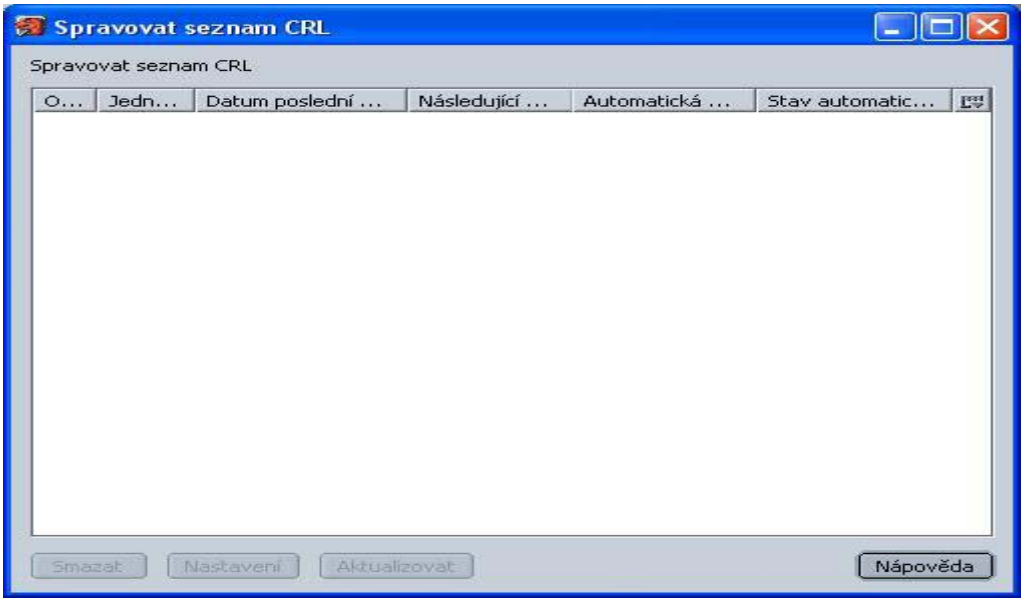
Mozilla umožňuje ověřovat platnost certifikátů dvojím způsobem – jednak pomocí CRL a jednak pomocí OCSP protokolu. Vzhledem k dobrým vlastnostem protokolu OCSP jej doporučujeme využívat. Protokol OCSP vrací na základě dotazu na platnost certifikátu okamžitou odpověď (jednu z možností : platný, neplatný, problém s určením výsledku). V tom je zásadní rozdíl proti ověřování proti CRL. Při použití CRL vlastně ověřujeme zda certifikát byl platný v době vydání CRL, nikoliv v době kdy jej ověřujeme (tato nevýhoda je zvláště výrazná, pokud CRL jsou vydávána s dlouhou časovou periodou). Proto zákon o elektronickém podpisu pro vydavatele kvalifikovaných certifikátů vyžaduje vydávání CRL nejpozději 1x za 12 hodin. Defaultně není protokol OCSP vybrán. b

Doporučujeme proto vybrat volbu *„ používat OCSP pro ověření platnosti těch certifikátů, které obsahují adresu služby OCSP“.*

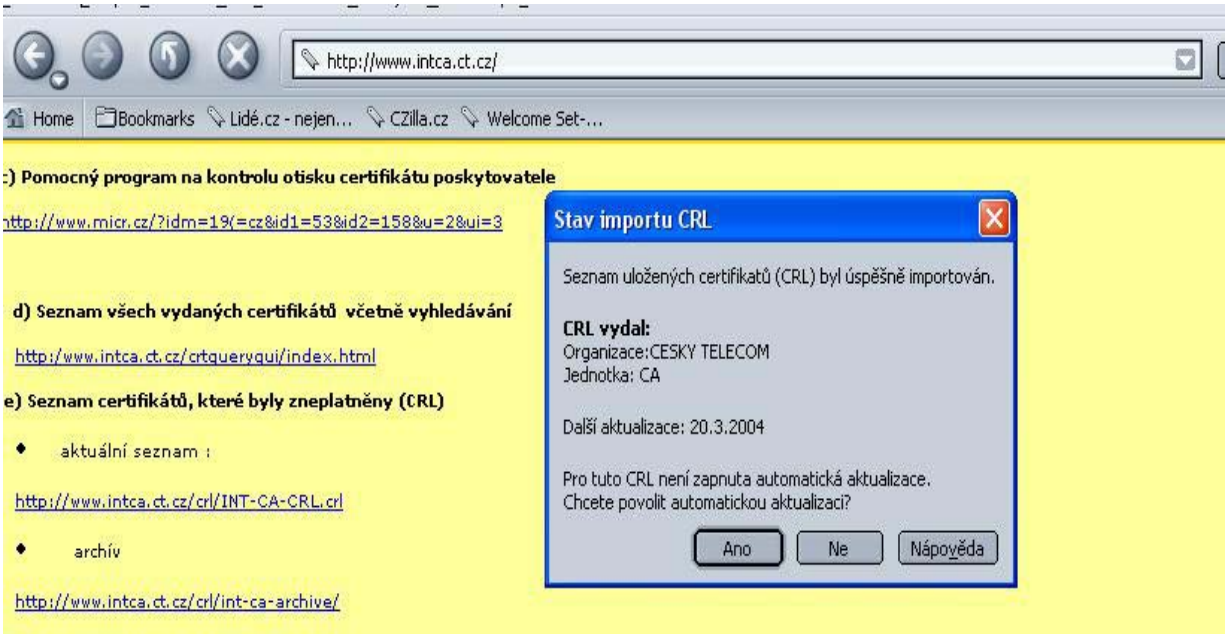
Třetí z možností má uplatnění pro specifická využití (např. pro přístup ke společným informacím o odvolání certifikátů více poskytovatelů v tzv. „bridge“ nebo v případě, že

administrátor informačního systému zpřístupní v rámci jím spravovaného systému informace o odvolání na jiné adrese než je uvedena v certifikátu atd.).

Dále zvolte *Spravovat seznam CRL*. V okně, které se otevře pravděpodobně nemáte žádné záznamy. Po instalaci prohlížeče Mozilla není totiž nastaveno stahování žádných CRL – tedy ani od přednastavených poskytovatelů certifikačních služeb. Uživatel si proto musí stahování CRL od vybraných poskytovatelů nastavit sám.

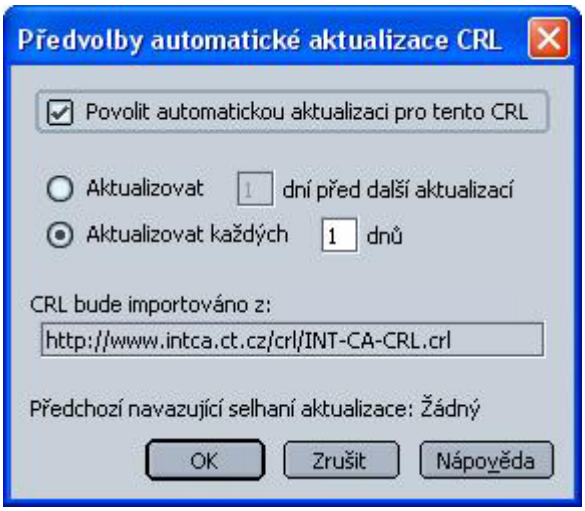


K tomu potřebujete příslušné CRL vyhledat (cestu k němu naleznete v certifikátech příslušného poskytovatele nebo na www stránce příslušného vystavitele). Předvedeme si celý postup na CRL, které vydává Interní certifikační autorita ČESKĚHO TELECOMU. Stránka autority je na adrese http://www.instca.ct.cz a CRL je zde v sekci certifikáty. Vyhledejte zde aktuální CRL a po jeho volbě (kliknutí na něj myší) se zahájí automaticky proces jeho stažení a uložení v aplikaci Mozzilla. V okně, které se objeví, jsme informováni o úspěšném importu.

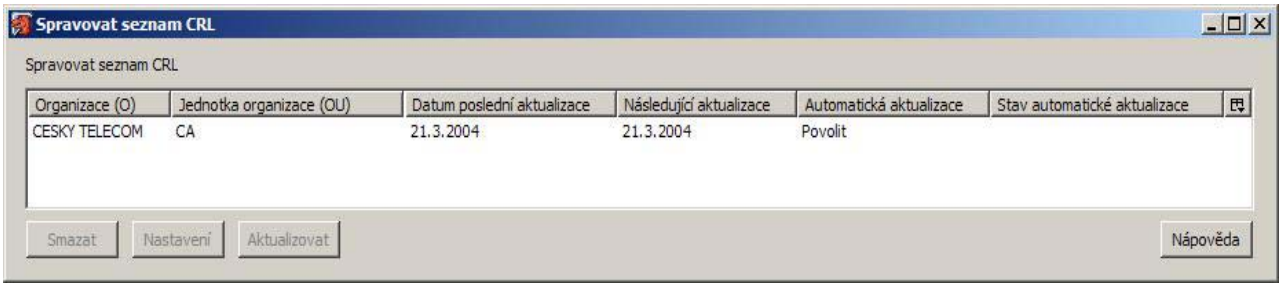


Nyní máte možnost nastavit automatické stahování a implementaci tohoto CRL. Tuto volbu doporučujeme, neboť se již dále sami nemusíte starat o aktualizaci tohoto seznamu. Připomeňme, že např. Internet Explorer obdobnou možnost nemá a uživatel musí opakovaně příslušná CRL od jím zvolených poskytovatelů stahovat a instalovat nebo k tomu musí využít pomocný program některé třetí strany.

Po volbě *Ano* se objeví předvolby pro automatickou aktualizaci pro toto konkrétní CRL. Cesta k CRL je již přednastavena. Doplňte *Povolit automatickou aktualizaci pro tento CRL* a podle periody vydávání CRL zvolte, kdy se má CRL aktualizovat. Nejmenší možná jednotka je 1 den. Potom zvolte *OK* a předvolby se uloží a začnou být ihned aktivní.



Podíváte-li se nyní do okna *Spravovat seznam CRL,* budou zde již k dispozici aktualizované informace. V našem případě to bude informace o tom, že máte staženo CRL ČESKÉHO TELECOMU a že je toto CRL pravidelně 1x denně aktualizováno. V praxi to znamená, že při kontrole certifikátů, které certifikační autorita ČESKÉHO TELECOMU vydala se kontroluje, zda nejsou uvedeny v CRL (ČESKÝ TELECOM neposkytuje OCSP přístup – jinak by měl tento způsob – vzhledem k námi provedenému nastavení přednost).



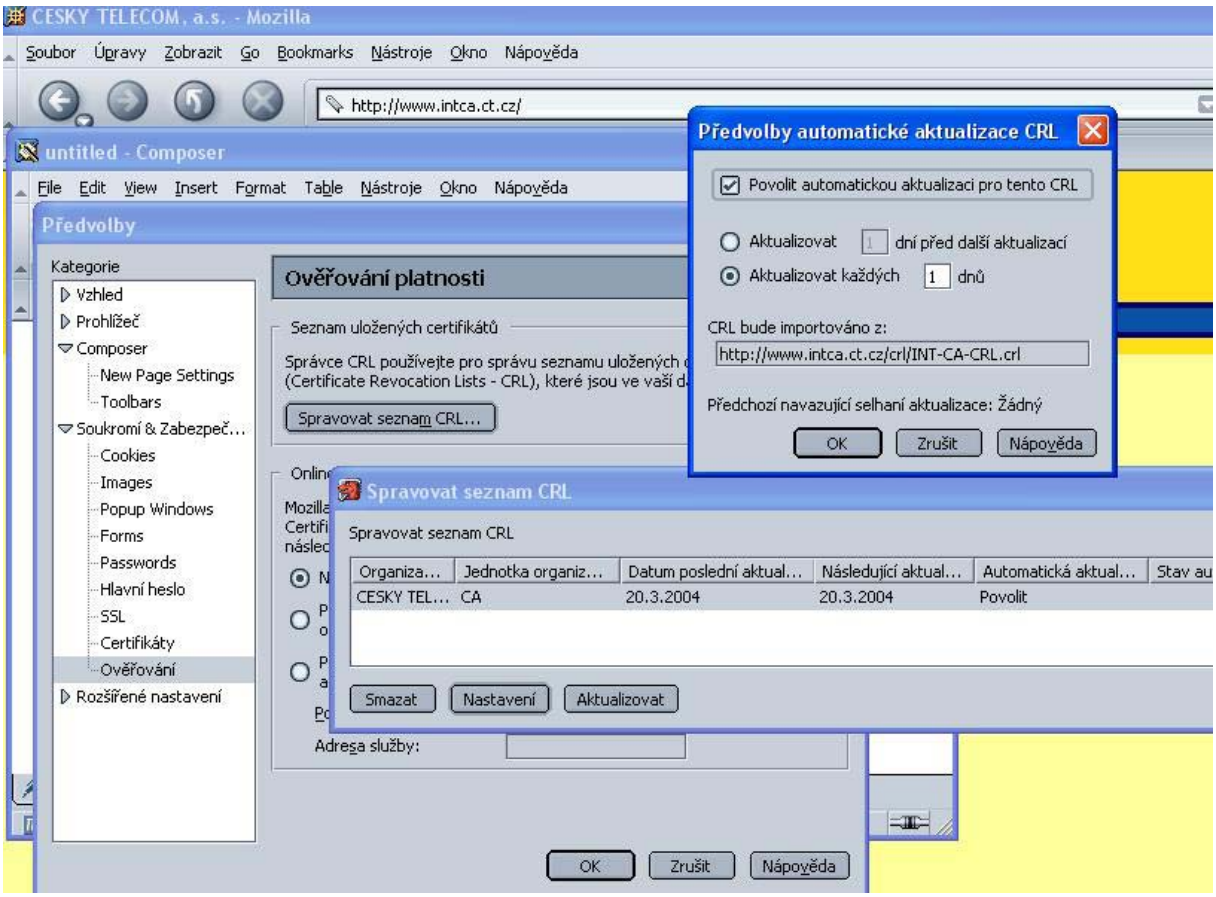
Obdobně doplňte stahování CRL dalších poskytovatelů certifikačních služeb, kde vám při ověření jimi vydaných certifikátů záleží na tom, aby bylo provedeno i ověření, zda byly zneplatněny.

Ze znění paragrafu 5 Zákona o elektronickém podpisu č.227/200 Sb. vyplývá, že subjekty, které se spoléhají na kvalifikované certifikáty by měly *provést vše možné*, aby ověřily jeho platnost tj. měly by při jeho ověření určitě používat CRL, a proto byste měli o poskytovatelů, kteří vydávají kvalifikované certifikáty toto nastavení rozhodně provést.

Obdobně můžete postupovat při **kontrole** zda máte nastaveno ověření certifikátů pomocí CRL a zda máte nastaveno jeho automatické stahování. V Mozille zvolte *Okno* a v roletovém menu vyberete Editor. V novém okně se otevře zvolený modul Editor. V jeho horní liště vyberete nabídku *Edit* a konečně v roletovém menu, které se otevře, vyberete *Předvolby*. Zde se v levém sloupci objeví položky, které lze v předvolbách nastavit. Pokud nejsou v levé části pod položkou *Soukromí & Zabezpečení* vidět žádné podkategorie, klikněte dvakrát na tuto kategorii a rozbalí se vám seznam možností. Potom vyberte možnost *Ověřování*.

Zobrazí se *Ověřování platnosti,* zde klikněte na *Spravovat seznam CRL*.

V okně, které se otevře, uvidíte seznamy CRL, které jsou v rámci vašeho nastavení Mozzily spravovány. Odtud můžete příslušný seznam A*ktualizovat* nebo se podívat na jeho konkrétní *Nastavení* a můžete zde také povolit nebo zrušit automatickou aktualizaci nebo upravit hodnoty příslušných parametrů.



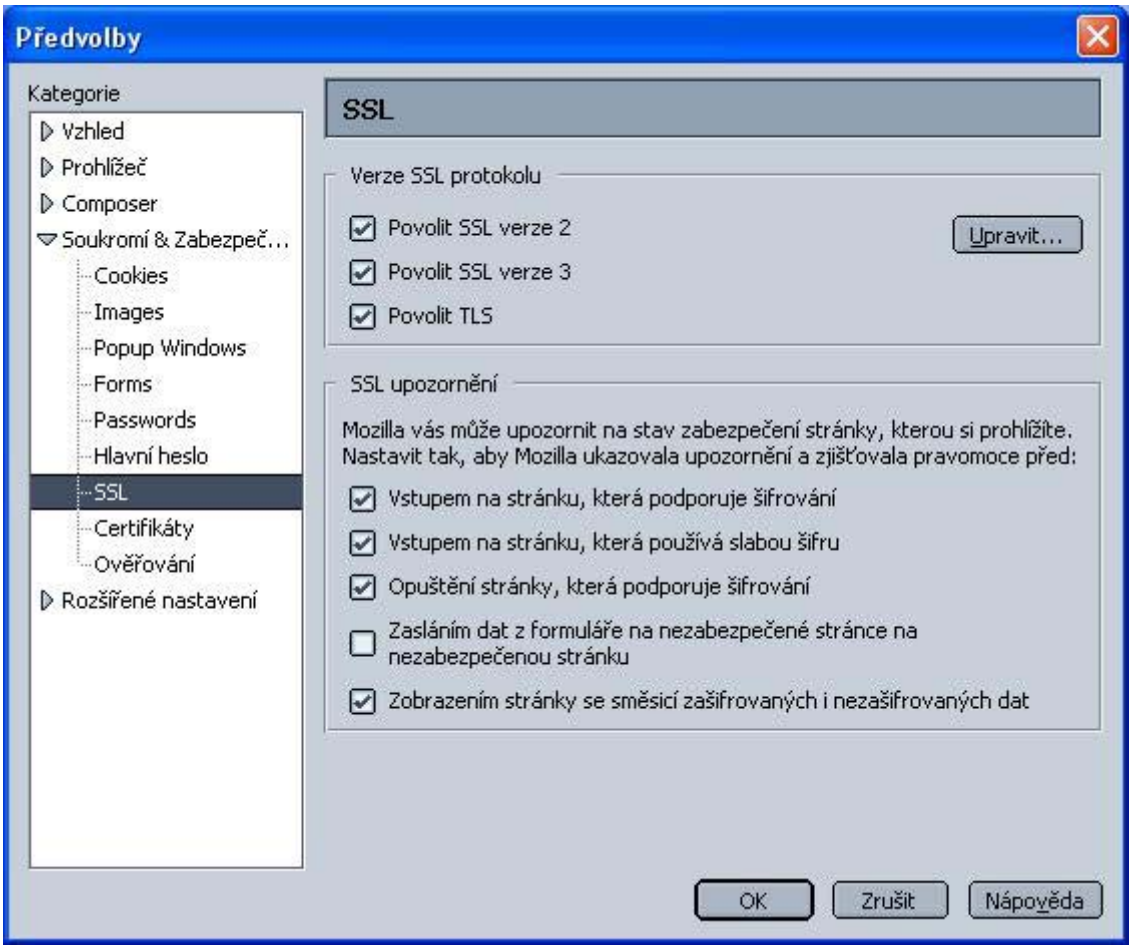
Celkový postup této kontroly je zobrazen na doprovodném obrázku.

Nastavení SSL komunikace v Mozille

Závěrem ještě ověřte, zda máte správně nastavenu SSL komunikaci ve vašem prohlížeči. Parametry SSL komunikace se nastavují v modulu *Soukromí & Zabezpečení* v kategorii SSL.

V Mozille zvolíte *Okno* a v roletovém menu vyberete Editor. V novém okně se otevře zvolený modul Editor. V jeho horní liště vyberete nabídku *Edit* a konečně v roletovém menu, které se otevře, vyberte *Předvolby*. 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 *SSL*.

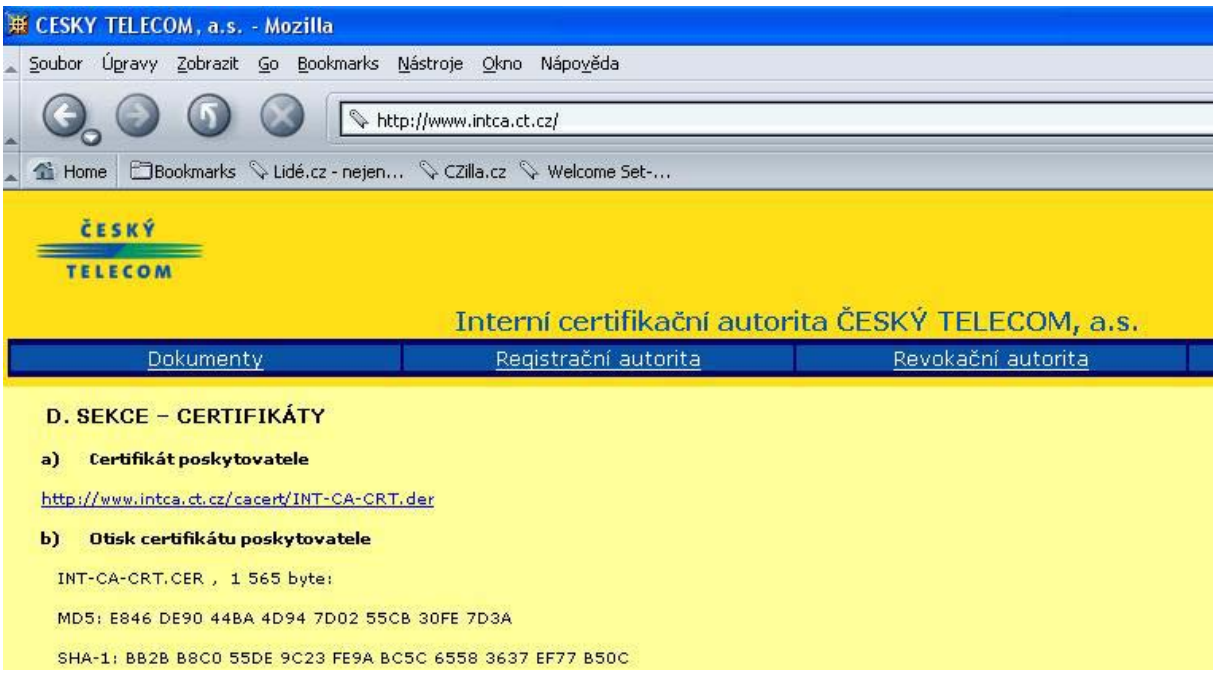
Doporučené nastavení je následující:



Volbu uložíte tlačítkem *OK*.

Stažení certifikátu poskytovatele na disk

Jak jsme se již zmínili, před instalací certifikátu poskytovatele je potřeba certifikát uložit na disk. Stažení kořenového certifikátu poskytovatele si ukážeme na následujícím příkladě. Nejprve se připojte na stránku poskytovatele a zde jeho certifikát vyhledejte (v případě Interní certifikační autority jej najdete na http://www.intca.ct.cz/ v sekci certifikáty.

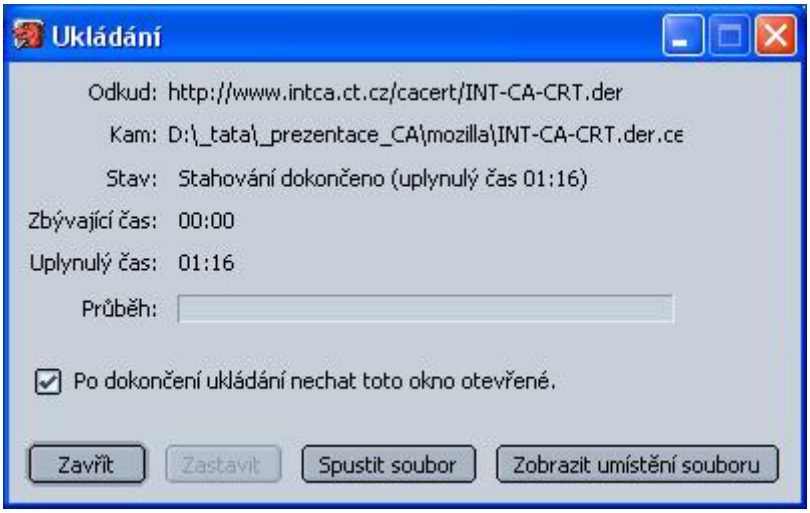


Je-li zde certifikát uložen ve více formátech, zvolte formát der resp. cer. Po kliknutí myší na odkaz, který vede k tomuto certifikátu, se objeví následující výzva :

V případě volby *Otevřít s výchozí aplikací (CERFile)* se vám otevře prohlížeč, který je součástí systému Windows. V tomto prohlížeči si můžete příslušný certifikát a jeho položky prohlédnout. Případně lze porovnat otisk (miniatura), který prohlížeč pro certifikát spočte s otiskem, který jste získali jiným důvěryhodným způsobem. V našem příkladě jsou otisky certifikátu poskytovatele na příslušné stránce také uvedeny. Dejte pozor - pokud byste nyní zvolili v prohlížeči certifikátu volbu *Instalovat,* certifikát by se nainstaloval do kořenového

úložiště, které využívají produkty firmy Microsoft tedy např. internet Explorer. Mozilla však má své vlastní úložiště a instalace certifikátů musí proběhnout způsobem, který byl již popsán dříve.

Abyste mohli certifikát nainstalovat do úložiště certifikátů Mozilla musíte jej uložit nejprve na svůj pevný disk, a proto zvolte *Uložit soubor na disk*.



Po uložení certifikátu na disk jsme o tom informováni v okně. Nyní můžete přejí k instalaci certifikátu do úložiště certifikátu programu Mozilla.

Závěr

Teprve po provedení všech výše uvedených postupů máte zajištěno, že při vstupu na www stránku, která je zabezpečena certifikátem od poskytovatele, kterému důvěřujete (máte jeho kořenový certifikát vědomě uložen v úložišti programu Mozilla) je provedeno řádné ověření zde uloženého certifikátu, včetně kontroly, zda není zneplatněn (tedy není uveden na CRL, které automaticky pravidelně na svůj počítač stahujete) a po té je zahájena důvěryhodná SSL komunikace mezi vaším počítačem a zabezpečeným serverem.

D. Zabezpečenie rozvoja elektronického podpisu v štátnej správe (Národný bezpečnostný úrad www.nbusr.sk)
(Materiál na medzirezortné pripomienkovanie (30.4.-14.5.04))
http://www.nbusr.sk/EP/material.rtf

1. Úvod

Zákon 215/2002 Z.z.. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) v § 10 definuje Národný bezpečnostný úrad ako Ústredný orgán štátnej správy pre elektronický podpis. Elektronický podpis je významným prvkom bezpečnosti v oblasti elektronickej komunikácie, najmä v podmienkach štátnej správy.

Zákon je naplnením smernice EÚ č. 1999/93/EC o elektronickom podpise v podmienkach SR. Samotná smernica ukladá povinnosť jej revízie v termíne júl 2003. Výsledky neboli doteraz zverejnené. Dá sa predpokladať, že po ich zverejnení a po zohľadnení skúseností s realizáciou zákona o elektronickom podpise bude potrebné zákon novelizovať.

Do uvedeného kontextu zapadá aj projekt IDA pre oblasť výmeny dokumentov v rámci administratívneho styku medzi orgánmi štátnej správy krajín EÚ, ku ktorému sa SR pripojila. Projekt predpokladá vybudovanie tzv. Bridge CA – certifikačnej autority, na ktorú sa budú pripájať národné certifikačné autority.

2. Zabezpečenie úloh, vyplývajúcich zo zákona pre NBÚ

Použitie elektronického podpisu v štátnej správe je podľa zákona podmienené existenciou akreditovaných certifikačných autorít. Podľa § 10 odseku 2) písmeno c) zákona Úrad vydáva kvalifikované certifikáty verejných kľúčov ním akreditovaným certifikačným autoritám. Z tohto dôvodu je Úrad povinný zriadiť koreňovú certifikačnú autoritu (KCA), ako najvyššiu štátnu autoritu, ktorá je z hľadiska dôvery nadriadená akreditovaným certifikačným autoritám.

Vybudovanie základnej funkcionality KCA bolo uskutočnené mimoriadne rýchlo s ohľadom na termíny úloh, ktoré ukladal zákon (vypracovanie vyhlášok, výber a inštalácia technológie, príprava na akreditáciu certifikačných autorít, organizačné a personálne zabezpečenie). Realizácia etapovitého budovania KCA, v súlade s dohodou s MF SR, nebola však doteraz dokončená v dôsledku nedofinancovania pôvodného zámeru. V súlade so závermi bezpečnostného auditu hlavnými nedostatkami sú chýbajúce záložné pracovisko a nedostatočné personálne zabezpečenie.

Požiadavka NBÚ na zabezpečenie kapitálových prostriedkov pre dobudovanie KCA nebola v štátnom rozpočte na rok 2004 zohľadnená. Vznikla tým krízová situácia pri plnení úloh NBÚ, vyplývajúcich zo zákona, s reálnym ohrozením znemožnenia využívania elektronického podpisu v informačných systémoch orgánov štátnej správy, ale aj prevádzky akreditovaných certifikačných autorít.

V prevádzke KCA chýbajú tabuľky pre 15 technických pracovníkov v dôsledku čoho sa porušujú ustanovenia zákona o bezpečnej prevádzke systému a nepretržitá prevádzka je zabezpečovaná iba v núdzovom režime bez záruky na spoľahlivosť.

Podľa § 20 ods. 5 je Úrad povinný zabezpečiť platnosť elektronického podpisu v prípade zániku akreditovanej certifikačnej autority. Toto ustanovenie je mimoriadne dôležité z hľadiska dlhodobej platnosti, vierohodnosti a bezpečnosti elektronického podpisu. Riešenie, ktoré prijal NBÚ pre zabezpečenie tejto úlohy v maximálnej miere využíva prostriedky KCA. Jej doplnením vzniká štruktúra, ktorá plní úlohy z hľadiska dlhodobej platnosti elektronického podpisu a ktorá môže byť využitá aj ako akreditovaná certifikačná autorita (ACA) pre interné potreby NBÚ ako ústredného orgánu štátnej správy.

Dôsledkom zastavenia výstavby uvedených technológií bude obmedzenie funkčnosti a zníženie bezpečnosti elektronického podpisu pri plnom nábehu aplikácií už v roku 2004 (daňové a colné aktivity, register obyvateľstva, vodičské preukazy a ďalšie aplikácie) a znemožnenie overenia elektronického podpisu, čiže nemožnosť určiť platnosť a pravosť rozhodnutí, vydaných štátnymi orgánmi v budúcnosti.

3. Prostredie elektronického podpisu v Slovenskej republike

V súčasnosti v Slovenskej republike pôsobí päť certifikačných autorít z toho jedna certifikačná autorita bola akreditovaná. Ďalšia certifikačná autorita je v procese akreditácie a dve certifikačné autority predbežne ohlásili podanie žiadosti o akreditáciu. Z tohto pohľadu, odhliadnuc od riešiteľných technických a legislatívnych problémov, je prostredie v SR pripravené pre nasadzovanie elektronického podpisu. Postupne bude treba doriešiť spomínané dofinancovanie KCA a jej personálne zabezpečenie, napojenie sa na EÚ a teda využívanie elektronického podpisu v medzinárodnom styku, najmä uznateľnosť zahraničných certifikátov v SR a certifikátov vydaných v SR v zahraničí.

Na základe signálov z praxe Asociácia Slovenska pre informačné technológie v spolupráci s Ministerstvom dopravy, pôšt a telekomunikácií SR a Národným bezpečnostným úradom iniciovala proces jednoznačného doriešenia rovnocennosti elektronických a papierových dokumentov a elektronických a vlastnoručných podpisov.

V súčasnosti prebieha proces prípravy realizácie úloh z uznesenia vlády SR č. 43/2004 k Stratégii informatizácie spoločnosti v podmienkach SR a Akčného plánu, ktoré vyplývajú z predvstupových záväzkov SR a je priamo napojené na zámery EÚ, vyjadrené v Akčnom pláne eEurope 2005. Uznesenie ukladá NBÚ rad úloh vo väzbe na jeho kompetencie v oblasti elektronického podpisu. Prioritnými oblasťami použitia elektronického podpisu je štátna a verejná správa a elektronický obchod, čo je plne v súlade s prioritami EÚ. Plnenie citovaného uznesenia vlády SR v týchto oblastiach predpokladá úzku spoluprácu predovšetkým MDPT SR, NBÚ, MV SR, MH SR a ďalších ústredných orgánov štátnej správy. Základným predpokladom však je schopnosť NBÚ plniť úlohy, vyplývajúce zo zákona o elektronickom podpise.

4. Spolupráca s MF SR, MV SR, NR SR

Prostredie pre zabezpečenie elektronického podpisu, ktoré vybudoval NBÚ, umožňuje vydávať kvalifikované certifikáty v zmysle zákona o elektronickom podpise akreditovaným certifikačným autoritám a pre vnútorné potreby NBÚ. Vzhľadom na skutočnosť, že certifikačná autorita, ktorá je súčasťou riešenia podľa požiadaviek zákona je využiteľná len za predpokladu zániku akreditovanej certifikačnej autority, javí sa účelným jej efektívne využitie i pre potreby iných ústredných orgánov štátnej správy. V praxi to znamená, že NBÚ je zo zákona povinný realizovať a prevádzkovať akreditovanú certifikačnú autoritu, ktorá bude použitá len za predpokladu zániku ním akreditovanej certifikačnej autority, čo z hľadiska pravdepodobnosti teoreticky nemusí nastať.

Zákon taxatívne neukladá NBÚ povinnosť vydávať kvalifikované certifikáty pracovníkom ústredných orgánov štátnej správy. Preto NBÚ neuvažoval s využitím tejto služby. Na základe požiadaviek rezortov a iných orgánov (Ministerstvo vnútra SR, Ministerstvo financií SR, Národná rada SR a pod.), ktoré vychádzajú hlavne z nutnosti garancie bezpečnostných aspektov u nich prevádzkovaných informačných systémov v nadväznosti na plnenie záväzkov voči EÚ, vysokej finančnej a personálnej náročnosti vybudovania akreditovanej certifikačnej autority a jej prevádzky, NBÚ analyzoval možnosť využitia existujúceho prostredia pre ich potreby tak, aby plne pokryl ich požiadavky na všetky typy certifikátov, ktoré tieto rezorty a orgány potrebujú na zabezpečenie svojich činností, spojených s elektronickým podpisom.

Najväčším problémom nie sú, ako by sa to na prvý pohľad javilo, prvotné investičné náklady (i keď tie predstavujú až niekoľko desať miliónové náklady), ale náklady spojené so správou, prevádzkou, splnením a riešením bezpečnostných aspektov, kladených na tieto certifikačné autority a problémy, spojené so získaním kvalifikovaného personálu.

NBÚ je schopný zabezpečiť využitie akreditovanej certifikačnej autority pre uvedené inštitúcie. Predpokladom je dobudovanie technológie a personálneho zázemia. Treba však dodať, že toto dobudovanie súvisí vo veľkej miere so zabezpečením podmienok, ktoré ukladá zákon tak, ako bolo uvedené vyššie a v minimálnej miere s uspokojením nárokov zmienených inštitúcií.

V súčasnosti mnohé rezorty stoja a v blízkej budúcnosti budú stáť pred nutnosťou budovania CA pre svoje potreby. Je na koncepčnom rozhodnutí vlády SR, či tento problém bude riešený izolovane (t.j. do určitej miery chaoticky z hľadiska kompatibility a so zvýšenými finančnými nákladmi) v rámci každej zložky alebo rozšírením už existujúceho technického, organizačného a personálneho vybavenia NBÚ, ktoré neznamená nutnosť zásadného navýšenia prostriedkov.

5. Stanovisko Protimonopolného úradu SR

Poskytovanie certifikačných služieb Národným bezpečnostným úradom bude realizované bezplatne výhradne len pre vnútornú potrebu štátnej správy, resp, menovaných rezortov a orgánov. Použitie certifikátov mimo túto oblasť nebude prípustné a z tohto dôvodu sa nepredpokladá zasahovanie do konkurenčného prostredia súkromnej sféry. Vzhľadom na povahu problému poskytovania kvalifikovaných certifikátov ústredným orgánom štátnej

správy bol tento zámer konzultovaný s Protimonopolným úradom SR. Jeho stanovisko je nasledovné:

Protimonopolný úrad SR, na základe informácií predložených zástupcom NBÚ, zaujal k vyššie uvedeným skutočnostiam nasledujúce stanovisko. Podľa názoru úradu vydávaním bezplatných certifikátov pre štátne orgány zo strany NBÚ by nemalo dôjsť k porušeniu zákona č. 136/2001 Z. z. o ochrane hospodárskej súťaže, resp. budúcich právnych noriem upravujúcich túto oblasť. Prípadné obmedzenie súťaže vyplývajúce zo špecifického postavenia NBÚ v rámci tejto činnosti prevážia prínosy tohto systému spočívajúce predovšetkým v ušetrení finančných prostriedkov štátu. Stanovisko úradu vychádza z predpokladu, že NBÚ nebude vydávať certifikáty fyzickým osobám, resp. podnikateľským subjektom.

6. Záver

V období od prijatia zákona o elektronickom podpise bol vybudovaný základ prostredia, umožňujúci jeho používanie. Nepokrytie kapitálových výdavkov rozpočtom roka 2004 pre NBÚ na vybudovanie aspoň základnej funkcionality záložného pracoviska KCA vytvorilo krízovú situáciu pri nasadzovaní elektronického podpisu v SR.

Na základe finančnej analýzy podľa prílohy tohto materiálu je NBÚ schopný mimo zabezpečenia tých úloh, ktoré mu vyplývajú s platnosti zákona, zabezpečiť certifikačné činnosti aj pre potreby vybratých ústredných orgánov štátnej správy.

Na zabezpečenie týchto úloh je požadované od ministerstva financií SR:

1. Vyčleniť mimo rozpočet pre rok 2004 sumu 8,7 mil. Sk na vyfinancovanie časti – kapitálové požiadavky pre KCA v celkovej sume 8,7 mil. Sk.

2. Zabezpečiť vyčlenenie požadovaných finančných prostriedkov pre roky 2005 až 2008 tak, ako sú požadované v bode 2. prílohy.

3. Vyčleniť mimo rozpočet pre rok 2004 čiastku 0,95 mil. Sk podľa rozpisu v bode 8. prílohy.

V prípade nesplnenia požiadavky podľa bodu č. 1 a č. 2 NBÚ nebude schopný plniť úlohy vyplývajúce z § 14 ods. 1, písm. a) a b) a §20 ods. 5 zákona č. 215/2002 Z.z. o elektronickom podpise, § 9 ods. 1, písm. d) vyhlášky NBÚ č. 541/2002 Z.z., § 13 vyhlášky NBÚ č. 541/2002 Z.z., § 3 ods. 3 a ods. 4 vyhlášky NBÚ č. 540/2002 Z.z..

V prípade nesplnenia požiadavky podľa bodu č. 3 NBÚ nebude schopný zabezpečiť požiadavky štátnej správy na bezplatné poskytovanie certifikátov od NBÚ a zložky štátnej správy budú nútené si tieto certifikačné činnosti zabezpečovať vlastnými certifikačnými autoritami, prípadne podnikateľskými subjektami. Týmto pádom v konečnom dôsledku vznikne SR v krátkodobom aj dlhodobom horizonte finančná strata , tak ako je analyzovaná v prílohe tohto materiálu.

Zabezpečenie prostriedkov na etapovité dobudovanie KCA v rokoch 2004-2008 umožní poskytovať služby pre ústredné orgány štátnej správy s vysokou mierou bezpečnosti a efektívnosti a umožní prepojenie na systémy EÚ.

E. Zmysel koreňovej certifikačnej autority

Ing. Radimír REXA, CSc. (R.Rexa@e-unicom.sk)
http://www.e-unicom.sk/forum/forum.asp

Diskusní príspevok k materiálu :
Zabezpečenie rozvoja elektronického podpisu v štátnej správe

Doterajšie náklady vynaložené na vybudovanie koreňovej certifikačnej autority KCA na Slovensku vo výške približne 100 miliónov Sk a ďalšie náklady plánované na jej dobudovanie a prevádzku v priemernej výške 60 miliónov Sk/rok bude rozumnejšie investovať do efektívnejších aktivít spojených so zavádzaním e-podpisu na Slovensku. Tou prvou by mala byť **novela zákona č. 215/2002 Z.z**. (ďalej Zákon) v záujme jeho harmonizácie s legislatívou EÚ a **presun dohľadu** nad týmto zákonom z branno-bezpečnostných štruktúr štátu do civilného sektora tak, ako je tomu v **ostatných krajinách EÚ**.

S ohľadom na neopodstatnenosť KCA na Slovensku do budúcnosti, čo vyplýva z priloženého vysvetlenia (viď príloha), bude vhodné prehodnotiť odhad dopadov na verejné financie, ako aj ďalšie údaje a podporné stanoviská uvedené v materiáli NBÚ. Prípadný presun investícií, doposiaľ vložených na zriadenie KCA, do prípadnej certifikačnej autority (CA, resp. ACA po získaní akreditácie) určenej výhradne pre potreby štátnej správy tak, ako je navrhované v predloženom materiáli, je potrebné riešiť s ohľadom na zvyklosti v rámci EÚ a hlavne s ohľadom na pravidlá na ochranu hospodárskej súťaže. Poskytovanie certifikačných služieb je totiž aj podľa slovenského Zákona (§12 ods.2) podnikaním.

V každom prípade je potrebné odčleniť od Úradu pre elektronický podpis (ďalej Úrad), úlohou ktorého je kontrola a regulácia činností súvisiacich s elektronickým podpisom (§ 10 a 11 Zákona), podnikateľské aktivity. Môže totiž dochádzať ku konfliktu záujmov.

Zosúladenie základnej koncepcie e-podpisu na Slovensku s konceptom EÚ napomôže podstatne efektívnejšiemu rozvoju elektronického podpisu, ako aj samotnej elektronizácii Slovenska v rámci zjednotenej Európy.

Poznámka: Na nekompatibilitu slovenského modelu e-podpisu s modelom EÚ a nehospodárnosť pri investovaní do KCA bolo upozorňované [1, 2, 3, 4] už v čase legislatívneho procesu spojeného so Zákonom a súvisiacimi vyhláškami č.537-542/2002 Z.z. Upozorňovali na ňu tiež niektorí zahraniční odborníci v rámci **medzinárodnej odbornej konferencie** "Elektronický podpis - kľúč k moderným elektronickým službám".

Príloha: Čo je vlastne koreňová certifikačná autorita a na čo slúži?

Pri overovaní platnosti elektronického podpisu na báze digitálneho podpisu pomocou certifikátu verejného kľúča je potrebné vedieť, **či autorita**, ktorá certifikát vydala, je **dôveryhodná.** Takéto stanovisko dáva väčšinou Úrad. Existuje niekoľko spôsobov, ako toto stanovisko sprístupniť aj overovateľom elektronických podpisov:

- koreňová certifikačná autorita (KCA),

- dôveryhodné zverejnenie verejného kľúča,
- mostíková (Bridge) certifikačná autorita (BCA).

a/ Koreňová certifikačná autorita (KCA)

Úrad prevádzkuje zároveň tzv. Koreňovú certifikačnú autoritu, ktorá vydá certifikát verejného kľúča k odpovedajúcemu súkromnému kľúču, ktorým príslušná Úradom uznaná certifikačná autorita podpisuje ňou vystavené klientské certifikáty. Podľa analýzy, ktorú si nechala vypracovať Európska komisia, z kapitoly 3.8 vyplýva, **že iba 4 z 30 hodnotených európskych krajín majú** národnú KCA (Nemecko, Holandsko, Poľsko, Belgicko). Tento nízky počet súvisí s vysokými nákladmi na zriadenie a prevádzku KCA v porovnaní s prínosom takéhoto riešenia.

b/ Dôveryhodné zverejnenie verejného kľúča

Najlacnejším riešením je dôveryhodné zverejnenie verejného kľúča príslušnej certifikačnej autority. Napríklad v susednej Českej republike Úrad zverejnil odtlačok certifikátu verejného kľúča zatiaľ jedinej akreditovanej certifikačnej autority, a to vo Věstníku Ministerstva informatiky a na www stránkach tohto ministerstva. Osoba spoliehajúca sa na podpisy založené na certifikátoch od tejto autority si musí manuálne nainštalovať tento nadradený certifikát do svojho počítača. Overovanie podpisov od tohto momentu už robí automatizovane.

c/ Mostíková (Bridge) certifikačná autorita (BCA)

Z hľadiska vzájomného uznávania kvalifikovaných certifikátov v krajinách EÚ v súlade s článkom 7.1 Direktívy 1999/93/EC a z hľadiska automatizovaného overovania podpisov sa ukazuje najvýhodnejší tretí spôsob riešenia prostredníctvom mostíkovej certifikačnej autority BCA. Z iniciatívy Európskej komisie sa v rámci projektu IDA už takáto spoločná mostíková certifikačná autorita pre oblasť výmeny dokumentov v rámci administratívneho styku medzi orgánmi štátnej správy krajín EÚ pripravuje.

F. Letem šifrovým světem

S některými vybranými událostmi v oblasti bezpečnosti IT a v kryptologii se od začátku tohoto roku můžete seznámit v nově zavedené sekci NEWS, kterou najdete na stránce Crypto-Worldu (http://crypto-world.info/news/). Tyto novinky pro vás vyhledávají a případně stručně komentují Tomáš Rosa, Vlastimil Klíma, Jaroslav Pinkava , Libor Tvrdík a Pavel Vondruška.

Návštěvnost této rubriky se postupně zvyšuje. V současné době zaznamenáváme průměrně 80 návštěv denně. Zajímavé je, že až jedna třetina návštěv je z USA.

Pro ty, kteří používají RSS čtečku (RSS) a mají zájem pravidelně sledovat přidané novinky, jsme na stránku NEWS přidali RSS kanál.

Stručný výběr z přehledu novinek, které jsme zde od zveřejnění minulého čísla Crypto-Worldu do vydání tohoto zveřejnili (konkrétní odkazy naleznete v sekci news):

15.05.2004	Studie Evropské komise o stavu zapracování a plnění směrnice o elektronickém podpise
13.05.2004	Bezplatný test bezpečnosti PC připojeného na Internet
13.05.2004	Vyšlo nové číslo "občasníku" Cryptobytes
13.05.2004	Guide for the Security Certification and Accreditation of Federal Information Systems
13.05.2004	NIST SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
13.05.2004	NIST SP 800-38C Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
13.05.2004	Kvantová kryptografie pro bezpečnou distribuci klíčů
11.05.2004	Další postranní kanál – geometrie textu!
11.05.2004	Bezpečná obrazovka
08.05.2004	Tvůrce počítačového červa Saser zadržen
07.05.2004	Siemens S55 phones send unauthorized SMS messages
07.05.2004	Piráti a IRC
07.05.2004	Počítače vyzařují informaci i akusticky!
07.05.2004	Nový draft Long-Term Archive and Notary Services
06.05.2004	Jak se chránit před spyware
05.05.2004	Nový rekord v kvantové kryptografii
05.05.2004	Top Ten Viruses and Hoaxes in April 2004
03.05.2004	RFC 3713 - A Description of the Camellia Encryption Algorithm
30.04.2004	RSA-576 faktorizováno podruhé?
30.04.2004	Novela zákona o elektronickém podpisu se zdrží
29.04.2004	Bezkontaktní VISA v Malajsii
28.04.2004	Microsoft Security Update - RSS
28.04.2004	Eagle 64K Flash Module v1 obdržel certifikát dle FIPS 140-2
27.04.2004	Kvantová kryptografie
26.04.2004	Bankovní karta řízená hlasem
23.04.2004	Kvantová podoba klasických kryptosystémů
23.04.2004	Chyba v TCP protokolu - doplnění informace
22.04.2004	Znovuobjevení vážné slabiny TCP/IP
22.04.2004	„PRIMES in P“ a praktická kryptologie
21.04.2004	Překvapení, které uniklo pozornosti: AES pro utajovaná data!
21.04.2004	Vyřešena úloha diskrétního logaritmu ECC2-109
19.04.2004	Přehled současného stavu symetrických šifer, konkrétně blokových a proudových šifer

VIII. O čem jsme psali v květnu 2000 - 2003

Crypto-World 5/2000

+ příloha : J.Hrubý , soubor QNG.PS

Crypto-World 5/2001

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 5/2002

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

Crypto-World 5/2003

G. 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