Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 10/2002 **15. října 2002**

10/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese:
http://www.mujweb.cz/veda/gcucmp/

(380 e-mail výtisků)

Obsah : **Str.**

(články neprochází jazykovou korekturou)

A. Úvodní komentář

(Mgr. Pavel Vondruška - ČESKÝ TELECOM a.s., pavel.vondruska@ct.cz)

Vážení čtenáři,
toto číslo Crypto-Worldu 10/2002 je prakticky celé věnováno elektronickému podpisu. Důvodem jsou dvě malá výročí, která se k říjnu váží.

Prvním z nich je dvouletá účinnost zákona č.227/2000 Sb. o elektronickém podpisu a druhým je výročí přijetí prováděcí vyhlášky k tomuto zákonu – vyhlášky, kterou připravil Odbor elektronického podpisu Úřadu pro ochranu osobních údajů č.366/2001 Sb.

Základní informace k těmto právním předpisům

Zákon č.227/2000 Sb.
Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
Zdroj: http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

Soubor:	Z_227_2000.pdf (88 kB)
Datum přijetí:	29. června 2000
Datum vyhlášení:	26. července 2000
Datum účinnosti od:	1. října 2000
Sbírka částka:	68
Stránka:	3290 - 3297
Novelizován:	č. 226/2002 Sb.
Aktuální citace:	(Zákon c.227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb.)

Vyhláška č.366/2001 Sb.
Vyhláška ÚOOÚ 366/2001 Sb. (k Zákonu o elektronickém podpisu č.227/2000 Sb.)
(Vyhláška Úřadu pro ochranu osobních údajů ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu)
Zdroj : http://www.mvcr.cz/sbirka/2001/sb138-01.pdf

Soubor:	V_336_2001.pdf (210 kB)
Datum přijetí:	3. října 2001
Datum vyhlášení:	10. října 2001
Datum účinnosti od:	10. října 2001
Sbírka částka:	138
Stránka:	7878 - 7883

Při této příležitosti uvedu krátký přehled některých událostí, které souvisí s činností odboru elektronického podpisu a váží se k výše uvedeným právním předpisům.

Odbor elektronického podpisu vznikl na Úřadě pro ochranu osobních údajů v létě roku 2000. Zpočátku měl pouze tři zaměstnance. Od samého začátku stojí v čele tohoto odboru ředitelka Mgr. Dagmar Bosáková (dagmar.bosakova@uoou.cz). Odbor má v současné době (včetně administrativních pracovníků) devět zaměstnanců. Poté, co 1.října roku 2000 vstoupil v platnost Zákon o elektronickém podpisu, bylo hlavním úkolem odboru připravit prováděcí vyhlášku k tomuto zákonu. Tato vyhláška byla po mezirezortním řízení a projednání v legislativní radě vlády přijata v říjnu roku 2001 a vstoupila v platnost právě před rokem - 10.října 2001.

Pracovníci odboru zveřejnili na základě svého zmocnění ve Věstníku Úřadu celou řadu upřesňujících požadavků k této vyhlášce č.366/2001 Sb. (např. požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku**,** požadavky na kryptografické moduly atd.) a dále řadu vysvětlujících komentářů k jednotlivým paragrafům vyhlášky (např. k příloze č.2 vyhlášky, k ověření objektové bezpečnosti ve smyslu §4, k ověření bezpečnosti informačního systému pro certifikační služby ve smyslu §6, písm. c vyhlášky, doporučenou osnovu k certifikační politice a certifikační prováděcí směrnici atd.). Pracovníci také připravili řadu interních dokumentů a metodik, které slouží při rozhodování ve správním řízení o udělení akreditace k poskytování certifikačních služeb a vyslovení shody nástrojů elektronického podpisu s požadavky uvedenými ve vyhlášce.

V následující tabulce je uveden seznam všech nástrojů, u nichž Úřad (Odbor elektronického podpisu) vyslovil (v souladu s § 8 odst. 3 vyhlášky č. 366/2001 Sb.) shodu. Aktuální informativní seznam je také zveřejňován na webových stránkách Úřadu pro ochranu osobních údajů.

Poř. čís.	**Nástroj elektronického podpisu**	**Výrobce**	**Věstník ÚOOÚ č.**
1.	**CSA8000;** Hardware Revision: G, Firmware Version 1.1, pracující ve FIPS módu	Eracom Technologies Australia, Pty. Ltd. Burleigh Heads Queensland Austrálie	15
2.	**nShield F3 SCSI;** Firmware 5.0, Hardware verze nC4032W-150, pracující ve FIPS módu	nCipher Corporation Ltd. Jupiter House Station Road Cambridge CBI 2JD United Kingdom	15
3.	**PrivateServer 3.0;** Firmware Version 3, Hardware Version 3.0, pracující ve FIPS módu	Algorithmic Research, Ltd. 10 Nevatim St., Kiryat Matalon Petah Tikva Israel	16
4.	**Luna CA^3 ;** Firmwarw verze 3.2.; hardware	Chrysalis-ITS, Inc. One Chrysalis Way Ottawa K2G6P9 Ontario	17

Pracovníci odboru dále ve správním řízení udělili akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb firmě **První certifikační autorita, a.s.** a to na základě:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona o elektronickém podpisu;
- splnění podmínek a požadavků stanovených vyhláškou č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu;
- splnění požadavků na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku zveřejněné v souladu s § 2 odst. 7 vyhlášky č. 366/2001 Sb;

- ověření kvalifikovaných certifikátů Úřadem pro ochranu osobních údajů podle § 10 odst. 7 zákona o elektronickém podpisu.

Aktuální informativní přehled udělených akreditací můžete nalézt na webových stránkách Úřadu pro ochranu osobních údajů v sekci elektronický podpis.

Pro účely ověření kvalifikovaného certifikátu akreditovaného poskytovatele certifikačních služeb (ve smyslu § 10 odst. 7 zákona č. 227/2000 Sb., o elektronickém podpisu) pracovníci odboru navrhli vlastní postup, který spočívá ve zveřejnění otisků certifikátů v všech poskytovatelem používaných formátech. Příslušná metodika i postup při ověření uživateli byly zveřejněny ve Věstníku Úřadu a vyloženy na odborných konferencích, kterých se pracovníci odboru zúčastnili.

Výsledek ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb První certifikační autority, a.s. zveřejnil Odbor elektronického podpisu na své webové stránce www.uoou.cz a ve Věstníku Úřadu č.17.

Poř. čís.	**Ověření kvalifikovaného certifikátu poskytovatele**				**Věstník ÚOOÚ č.**
	Subjekt:		Adresa:		
1.	**První certifikační autorita, a.s., identifikační č. 26 43 93 95**		**Podvinný mlýn 2178/6, PSČ 190 00 Praha 9**		**17**
V ý s l e d k y o v ě ř e n í :					
A.	Jméno:	**qica_root_cert_20020321.pem**	Délka: **2265**		Poslední změna: **22. 3. 2002** v **11:14** hod.
	Formát certifikátu:		**O t i s k :**		
	PEM	SHA-1	**4BFB ED36 68FC 2B0A B729 8EC0 53B5 3649 6E15 0AAE**		
		MD5	**297C 49A7 B63C B15A F3B7 0F45 2D3B 5132**		
B.	Jméno:	**qica_root_cert_20020321.der**	Délka: **1630**		Poslední změna: **21. 3. 2002** v **21:02** hod.
	Formát certifikátu:		**O t i s k :**		
	DER	SHA-1	**6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE**		
		MD5	**C3F3 5AB5 24C7 9276 634B 4DB4 E86A FE57**		
C.	Jméno:	**qica_root_cert_20020321.txt**	Délka: **6256**		Poslední změna: **22. 3. 2002** v **11:18** hod.
	Formát certifikátu:		**O t i s k :**		
	TXT	SHA-1	**AC46 FB40 E929 F12D 758A 0B8E 0192 516B 1B65 6C8A**		
		MD5	**5EAC 0082 F5F5 9E3D EAB4 0FE6 27BE 5ED2**		

Tyto zveřejněné otisky slouží k tomu, aby před instalací kvalifikovaného certifikátu akreditovaného poskytovatele certifikačních služeb byla možnost porovnáním otisků zjistit, zda:

- kvalifikovaný certifikát byl skutečně ověřen Úřadem,
- kvalifikovaný certifikát byl vydán příslušným akreditovaným poskytovatelem certifikačních služeb,
- se jedná o kvalifikovaný certifikát, kdy k němu odpovídající data pro vytváření elektronického podpisu daného akreditovaného poskytovatele certifikačních služeb jsou určena pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny.

Na webových stránkách Úřadu byl umístěn volně ke stažení program „DataHash“, který umožňuje výpočet otisků souborů pomocí hashovacích algoritmů MD5 a SHA-1. S pomocí těchto výsledků se lze ujistit, že uživatel nemá pozměněný certifikát akreditovaného poskytovatele.

Pracovníci odboru navrhli topologii testovací linky, která umožňuje testování a předvádění různých úkolů z oblasti nasazení elektronického podpisu. Tato linka byla postavena ve spolupráci s Katedrou systémového inženýrství MFF UK Praha (RNDr. Vojtěch Jákl, CSc., RNDr. Antonín Beneš, PhD.) a v únoru roku 2002 uvedena do provozu.

Celkově se skládá z pěti certifikačních autorit (typu standalone a enterprise), které tvoří tři různé nezávislé systémy.

První systém slouží pro úkoly, které pro ÚOOÚ vyplývají ze zákona o elektronickém podpisu (Zákon č.227/2000 Sb., §10 odst. 7, § 13 odst. 2, …).

Druhý systém tvoří certifikační autorita pro vydávání certifikátů zaměstnancům ÚOOÚ pro vnitřní komunikaci a potřeby odboru a úřadu.

Třetím systémem je testovací, školící a předváděcí linka. Jde o lokální síť, která se skládá z DNS serveru (Windows 2000 server) a MS Exchange serveru (Windows 2000 server). Další tři počítače jsou uživatelské stanice. Na první je nainstalován systém Windows 2000 a prohlížeče MS Explorer 5.0, Netscape 6.2, Opera 6.0. Druhá stanice je postavená na Windows XP s Office XP a MS Explorerem CZ 6.0. Na třetí stanici je Linux Red Hat 7.1 CZ, prohlížeč Opera 5.0 a Nestcape Navigator 4.77.

Správcem certifikační autority je Mgr. Vladimír Sudzina (vladimir.sudzina@uoou.cz). Linka slouží pracovníkům ÚOOÚ, ale i **zdarma** všem zájemcům z oblasti veřejné správy. Pracovníci odboru připravili řadu krátkých úkolů – tasků, které zde rádi předvedou resp. zaškolí příslušné zájemce o tuto problematiku. Nutná je předchozí domluva na volném termínu se správcem systému.

Pracovníci odboru dále vedli řadu konzultací s různými subjekty veřejné a komerční sféry. Snahou bylo (ve skromných podmínkách Úřadu) provádět i osvětovou a propagační činnost k tématu elektronického podpisu. Během let 2000-2002 pracovníci odboru (především ředitelka odboru Mgr.Dagmar Bosáková, Mgr. Pavel Vondruška a Bc.Jan Hobza) vystoupili na desítkách konferencí, seminářů a na zvaných přednáškách. Odbor uspořádal i půldenní seminář pro zájemce z řad novinářů, kde se snažil vysvětlit přístupnou formou základní pojmy zákona o elektronickém podpise a vysvětlit podstatu elektronického podpisu.

S touto činností úzce souvisí bohatá publikační činnost. V uvedeném období publikovali pracovníci odboru na 60 článků a příspěvků (včetně jedné knihy), které byly věnovány problematice elektronického podpisu.

Do kategorie osvětové činnosti odboru spadá i následující příspěvek („Elektronický podpis“) Bc. Jana Hobzy, který byl sestaven na základě jeho krátkých článků, které od jara 2002 vycházejí na pokračování v časopise Veřejná správa.

Věnování

Tento úvodní přehled věnuji svým kolegům jako poděkování za práci, kterou za tyto dva roky vykonali. Přeji jim touto cestou v dalších letech co nejméně překážek v jejich práci a radost z toho, co tak nadšeně budují.

Pavel Vondruška (do 30.9.2002 – Odbor elektronického podpisu, ÚOOÚ
od 1.10.2002 – ČESKÝ TELECOM a.s.)

B. Elektronický podpis

Mgr. Jan Hobza, ÚOOÚ

Obsah :

Trochu práva pro začátek

Kolotoč, který se u nás točí kolem elektronického podpisu již od roku 2000, má svůj původ v Evropské unii. Evropský parlament a Rada vydaly dne 13.12.1999 Směrnici o zásadách společenství pro elektronické podpisy, která ukládá členským státům přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Směrnice Evropského parlamentu jsou pro členské státy co do svých požadavků závazné, a tak by i Česká republika, jako kandidátská země, měla postupovat v souladu s těmito předpisy.

Zásadním požadavkem Směrnice je, aby kvalifikované elektronické podpisy (tj. elektronické podpisy založené na ”kvalifikovaných certifikátech” a vytvořené pomocí ”prostředků pro bezpečné vytváření podpisů”) splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě stejně, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k datům na papíře. Co to vlastně znamená? Tam, kde právní předpis umožňuje činit právní úkony i v elektronické podobě, kvalifikovaný podpis má mít stejné právní účinky (předpoklad platnosti právního úkonu). Tento požadavek je téměř revoluční, neboť rozšiřuje paradigma vnímání pojmu „listina“ (tj. fyzický nosič, na němž lze zachytit projev vůle a tedy i učinit právní úkon) o digitální formu.

Z tohoto požadavku nevyplývá, že veškeré právní úkony mají být platné, pokud je opatříme kvalifikovaným podpisem. Právní řády členských států, ale i náš právní řád, vyžadují pro různé oblasti práva různou formu a různé podmínky právního úkonu. A tak i kvalifikovaný elektronický podpis lze platně použít pouze tam, kde to zákon připouští.

Pokud tedy občanský zákoník stanoví, že „vlastnoruční závěť musí být vlastní rukou napsaná a podepsaná, jinak je neplatná“, nic Vám nepomůže elektronický podpis. Kde se tedy můžeme platně elektronicky podepisovat? Všude tam, kde to právní předpis dovoluje (respektive neimplikuje neplatnost nedodržením písemné formy). Jsou to tedy takové úkony, které činíme podle § 34 až 51 občanského zákoníku (např. spotřebitelské smlouvy, kupní smlouvy, ale i smlouvy o dílo apod.). Dále je možné platně elektronicky učinit podání podle správního řádu, zákona o správě daní a poplatků, občanského soudního řádu či trestního řádu.

Vytváření elektronického podpisu

V této části si řekneme, co všechno předchází vytváření a používání zaručeného elektronického podpisu.

První podmínkou je existence druhé strany, která bude schopna a ochotna naše elektronické podpisy přijímat, ověřovat a spoléhat se na ně. Jinými slovy musí mít adresát našich podepsaných emailů odpovídající počítačové vybavení, přístup k našemu certifikátu a možnost či právní povinnost se spolehnout na náš elektronický podpis. Takovým adresátem může být náš obchodní partner či finanční ústav nebo úřad státní správy. Ač se tato podmínka zdá být banální, představuje jedinou zásadní překážku širšího uplatnění elektronického podpisu. Pokud máme „partnera“, který odpovídá našim požadavkům, je zbytek starostí jen na nás.

Nejdříve si na internetu vybereme některého z poskytovatelů certifikačních služeb (zkráceně PCS). Na jeho stránkách pak dle instrukcí vyplníme žádost o osobní certifikát. Po odsouhlasení žádosti vygeneruje náš internetový prohlížeč dva digitální klíče, tajný a veřejný. Veřejný klíč potom připojí k naší žádosti o certifikát. Podle typu certifikátu pak žádost buď uložíme na disketu a fyzicky ji přineseme našemu PCS, nebo ji odešleme přes internet k vyřízení. Poskytovatel naši žádost zkontroluje, případně ověří naši totožnost a vytvoří nám certifikát. Na počítači, ze kterého jsme o certifikát žádali, nainstalujeme velice jednoduše tento náš certifikát. Tím se aktivuje i náš soukromý klíč, který až do té chvíle zůstával nedostupný. Nyní se již můžeme elektronicky podepisovat.

V našem emailovém klientovi ve složce „zabezpečení“ vybereme náš certifikát a zatrhneme možnost digitálně podepisovat. Pro větší pohodlí našeho partnera můžeme zatrhnout i odesílání našeho certifikátu spolu se zprávou. Další vytvořený email se již odešle elektronicky podepsaný.

Ověření elektronického podpisu

V tomto odstavci se podíváme právě k příjemci naší zprávy a řekneme si, jaké kroky musí uskutečnit k ověření našeho elektronického podpisu.

Pokud bude přenos naší zprávy úspěšný, našemu partnerovi se objeví ve složce doručená pošta nová položka. Že je daná zpráva elektronicky podepsaná, pozná již ze vzhledu ikony zprávy  . Po jejím otevření se v pravém horním rohu objeví ikona zástupce elektronického podpisu  . Kliknutím na pečeť se otevře okno s požadovanými

informacemi o elektronickém podpisu: zda zpráva nebyla po podepsání změněna, a zda certifikát podpisu je a) stále platný, b) nebyl zneplatněn a c) je důvěryhodný. To jsou náležitosti, které musí ověřit příjemce zprávy dle zákona o elektronickém podpisu.

Zda zpráva nebyla po podepsání změněna, neboli ověření integrity dokumentu, probíhá automaticky. Poštovní klient k tomu vyžaduje pouze dokument, elektronický podpis a certifikát podpisu, který bývá součástí zasílané zprávy. Automaticky probíhá i ověření platnosti certifikátu, neboť to se zjišťuje porovnáním současného datumu a období platnosti certifikátu.

K ověření, zda certifikát osoby nebyl zneplatněn se používá aktuální seznam zneplatněných certifikátů (tzv. CRL). Toto CRL (běžně ve formě souboru s příponou .crl) si musí příjemce pošty stáhnout z internetové stránky certifikační autority (CA), která certifikát vydala, a nainstalovat jej (jednoduše z nabídky vlastností tohoto souboru). Poštovní klient pak již sám ověří, zda zaslaný certifikát nefiguruje na tomto seznamu a zda tedy nebyl zneplatněn.

Posledním povinným ověřením je zjištění důvěryhodnosti certifikátu. Ta je zajištěna elektronickým podpisem certifikátu uživatele, který je součástí samotného certifikátu. Tento podpis vytváří certifikační autorita při generování certifikátu pro každého uživatele. Je tedy nasnadě potvrdit či vyvrátit důvěryhodnost certifikátu (jinými slovy zda certifikát nebyl podvržen) ověřením platnosti elektronického podpisu samotného certifikátu. K tomu je nutné stáhnou z internetové adresy certifikační autority její vlastní certifikáty a nainstalovat je do svého poštovního klienta (opět jednoduše z vlastností certifikátu). Pokud již certifikáty CA již v poštovním klientovi jsou, není nutné tento krok opakovat pro každou zprávu.

Nyní již náš partner udělal všechno nutné k ověření našeho elektronického podpisu a pokud nejsou některé z ověření negativní, může se na podpis spolehnout.

Technologie podepisování

Běžnému uživateli se může zdát, že technologie elektronického podpisu je velice jednoduchá. Uživatelské rozhraní je přívětivé a neklade na technické znalosti podepisující osoby větší nároky. A myslím, že by to tak i mělo být. Stačí jen nainstalovat certifikát, klinout na ikonu „elektronicky podepsat“ a je vyhráno. My si dnes ovšem trochu prohloubíme znalosti a podíváme se „pod povrch“ našich poštovních klientů.

K podepisování se používá jedinečné, velmi dlouhé číslo, kterému říkáme tajný kryptografický klíč. K ověřování podpisu, čili k ověření, zda zpráva nebyla po podepsání změněna, se používá veřejný kryptografický klíč. Oba klíče jsou spolu v matematické závislosti a mají takové vlastnosti, které zaručují, že není možné odvodit jedno ze druhého. Oba klíče se generují při vytváření žádosti o certifikát na Vašem PC (PC, ze kterého se budete podepisovat).

Po vytvoření žádosti o certifikát nám certifikační autorita vydá pro náš veřejný klíč certifikát. Instalací certifikátu do prohlížeče se aktivuje i náš tajný klíč. Nyní můžeme podepisovat.

Pro elektronický podpis se v běžných poštovních klientech používají tzv. asymetrické algoritmy schématu s dodatkem. To znamená, že soukromým klíčem nešifrujeme celou zprávu (nedochází tak k utajení jejího obsahu), ale jen její otisk, neboli „haš“. Haš je ve srovnání s původní správou velmi malé číslo, ze kterého není možné zpětně dovodit obsah dokumentu. Zároveň není možné pro týž dokument vypočítat stejnou funkcí jiný haš, tedy jeho jinou hodnotu. Tyto vlastnosti využijeme především v příštím čísle, kdy budeme ověřovat elektronický podpis.

Z dokumentu tedy nejdříve vypočítáme haš (k tomu se běžně používají hašovací funkce jako SHA-1 či MD5). Tento haš se následně zašifruje naším soukromým klíčem. Podle způsobu generování klíčů se jako šifrovací algoritmy většinou používají DSA, ECDSA, či RSA. Elektronický podpis je tedy zašifrovaný haš původní zprávy.

Uvedené operace, jako generování klíčů, vypočet haše a šifrování podpisu, většinou za Vás provádí CSP (crypto service provider), čili softwarový modul na Vašem PC.

Technologie ověřování

Náš partner, tak jak jsme se s ním předem domluvili, nám poslal elektronicky podepsaný email. Pokud tak učinil právní úkon, např. návrh smlouvy, bude pro její platné uzavření důležité, co podnikneme my. Ze zákona máme povinnost ověřit platnost elektronického podpisu a platnost certifikátu podepisující osoby. Jak ověření platností provedeme my již víme ze třetí kapitoly. Zde si popíšeme algoritmus ověřování elektronického podpisu z pohledu našeho poštovního klienta.

K ověření platnosti je nutné mít k dispozici původní dokument, elektronický podpis a certifikát podepisující osoby s odpovídajícím veřejným klíčem. Při ověřování podpisu se nejdříve z původního datového dokumentu vypočítá haš (jednoznačný otisk) pomocí stejné funkce, kterou použil náš partner při podpisu.

V druhém kroku je dešifrován elektronický podpis. Invertovaná asymetrická funkce aplikuje veřejný klíč z certifikátu na elektronický podpis. Běžně se předem kontroluje, zda veřejný klíč v certifikátu odpovídá soukromému klíči podepisující osoby. Pokud ano (když odesílatel zašle certifikát i se zprávou, tak vždy), bude výstupem funkce původní haš dokumentu. Porovnáním obou hašů (námi vypočteného a získaného dešifrováním podpisu) se zjistí, zda je elektronický podpis platný.

Pokud se při porovnávání zjistí, že haše nejsou shodné, je velice pravděpodobné, že zpráva byla po podepsání změněna. V takovém případě poštovní klient zobrazí varování o neplatnosti elektronického podpisu. Jsou-li oba haše shodné, je možné se na elektronický podpis spolehnout.

Zhruba takto probíhá ověření integrity datové zprávy a autentizace podepisující osoby. Ze zákona je však nutné ještě ověřit platnost daného certifikátu. Kromě kontroly, zda certifikát není uveden na seznamu zneplatněných certifikátů (viz. minulý díl), se provádí ještě ověření platnosti podpisu certifikátu. Stručně se dá říci, že výše uvedený postup pro ověření platnosti elektronického podpisu nějaké zprávy se obdobně aplikuje i pro ověření elektronického podpisu certifikátu. Veřejný klíč se tentokrát získá z certifikátu certifikační autority, který si příjemce pošty musí nainstalovat sám z důvěryhodného zdroje.

Pokud se Vám zdá výše uvedený postup poněkud nesrozumitelný či složitý, pak je to pouze omezeným rozsahem tohoto článku a nikoli autorem. Rozhodně však nemusíte mít obavy z přijímání elektronicky podepsané pošty, většinu práce za vás provede váš poštovní klient.

Akreditace

Ve výše uvedených kapitolách jsme používali pojem kvalifikovaný certifikát, aniž bychom předem definovali, jakou má váhu, či lépe, kdo jej může vydávat. Podle českého zákona o elektronickém podpisu mohou vydávat kvalifikované certifikáty (dále jen QC) dva typy subjektů. Jsou jimi poskytovatelé certifikačních služeb, kteří Úřadu pro ochranu osobních údajů **oznámili,** že hodlají vydávat QC, a pak to jsou tzv. **akreditovaní** poskytovatelé certifikačních služeb. Oba mohou pro veřejnost vydávat QC, na základě nichž lze platně podepisovat právní úkony podle občanského zákoníku. Některé právní úkony lze ovšem činit jen pomocí QC od akreditovaného poskytovatele. Těmito úkony jsou především podání činěná v oblasti orgánů veřejné moci.

Jak správně předpokládáte, mezi oběma poskytovateli existuje rozdíl nejen v názvech. Akreditovaný poskytovatel musí před získáním svého titulu zaplatit správní poplatek (v současné době 100.000,- Kč), předložit Úřadu bezpečnostní dokumentaci, doložit dostatečnost finančních zdrojů, předložit výsledek kontroly bezpečnostní shody, prokázat, že používá bezpečné nástroje elektronického podpisu a doložit splnění dalších povinností stanovených zákonem o elektronickém podpisu.

U poskytovatele certifikačních služeb, který splnil oznamovací povinnost, je postup poněkud odlišný. Jak v zahraniční praxi, tak i v českém pojetí se u takových poskytovatelů ověřuje splnění zákonných povinností ex post (obdoba auditní činnosti). Poskytovateli se tedy neuděluje povolení (licence) k výkonu této činnosti jako u akreditovaného poskytovatele. Stejný postup uplatňuje již určitou dobu i Německo.

Zákon o elektronickém podpisu rozlišuje i další povinnosti obou typů poskytovatelů certifikačních služeb, které pro náš seriál již nejsou natolik důležité. Měli bychom si však zapamatovat, že QC lze použít pro právní úkony podle občanského zákoníku a při komunikaci v oblasti orgánů veřejné moci je možné používat pouze QC od akreditovaného poskytovatele.

Standardy

Pro uživatele elektronického podpisu je bezpochyby důležité, aby technologie používané při generování klíčů a certifikátů, postupy při vytváření a ověřování elektronického podpisu a metody ověřování platnosti certifikátů, byly bezpečné. Určitou míru bezpečnosti je nutné zajistit i z důvodu, aby elektronický podpis dokázal splnit stejné požadavky, které klademe i na podpis vlastnoruční. Tento fakt si uvědomovali i tvůrci Směrnice ES o zásadách společenství pro elektronické podpisy.

Směrnice umožňuje Evropské komisi vytvářet standardy pro elektronické podpisy a zveřejňovat jejich čísla v oficiálním věstníku ES (EC Official Journal). Tento postup má několik výhod. Produkty, které budou splňovat požadavky zveřejněných standardů, se považují za vyhovující pro všechny členské státy EU. Není tedy třeba pro výrobce či

dodavatele podstupovat proces vyhodnocení jeho výrobku pro každý členský stát zvlášť. Tím je zajištěna i interoperabilita již vyhodnocených produktů pro elektronické podpisy na evropské úrovni. Jelikož i Česká republika se hlásí k implementaci Směrnice, tyto produkty by měly vyhovovat i požadavkům našeho právního řádu.

Samotní úředníci Evropské komise samozřejmě nemohou mít dostatečnou kvalifikaci k tomu, aby dokázali vytvořit odpovídající standardy pro elektronický podpis. Za tím účelem byla zřízena iniciativa EESSI (European Electronic Signature Standardization Initiative), jejíž členové si dali za cíl identifikovat hlavní oblasti pro tvorbu nových standardů. V červenci 1999 vydala EESSI pracovní program, který jako hlavní standardizační oblasti uvádí:

- používání kvalifikovaných certifikátů podle X509,
- formáty elektronických podpisů, důvěryhodné systémy certifikačních autorit a autorit časových razítek,
- certifikační politiky,
- profily pro vyhodnocování produktů pro elektronický podpis a
- metody vyhodnocování.

K plnění tohoto plánu bylo ve spolupráci s dalšími standardizačními orgány (ETSI a CEN) vytvořeno několik pracovních skupin. Každá z nich se soustředí na určitou oblast a od roku 2000 zveřejňuje k připomínkám své dokumenty. Vrcholem jejich snažení by měla být publikace standardů v oficiálním věstníku ES zhruba v roce 2003.

Certifikační politika

První akreditovaný poskytovatel začal před několika měsíci vydávat kvalifikované certifikáty pro elektronické podpisy. Každý občan tedy již může na základě smlouvy využívat certifikačních služeb akreditovaného poskytovatele. Podle zákona má tento poskytovatel povinnost písemně informovat žadatele o přesných podmínkách pro užívání kvalifikovaného certifikátu, včetně případných omezení pro jeho použití, a o podmínkách reklamací. Podstatné části těchto informací musí být na vyžádání k dispozici třetím osobám, které se spoléhají na tento kvalifikovaný certifikát. Je běžnou praxí tyto a další informace uvádět v dokumentu s názvem Certifikační politika. Prováděcí vyhláška též ukládá poskytovateli před udělením akreditace tento dokument zpracovat a předložit k posouzení.

Certifikační politika je svou povahou veřejný dokument. Z hlediska podepisující osoby a spoléhající se strany tvoří jeho hlavní kapitolu tzv. obecné zásady (general provisions – viz. RFC 2527 ftp://ftp.isi.edu/in-notes/rfc2527.txt). Poskytovatel certifikačních služeb v nich specifikuje, jaké povinnosti mají zúčastněné strany při využívání jeho služeb, jakým způsobem tyto služby realizuje a jakou kdo nese odpovědnost. Konkrétně se zde upravuje, pro jaké účely lze certifikáty vydávané podle této politiky používat, jakým způsobem se má chránit soukromý klíč, jak zažádat o zneplatnění certifikátu a podobně. Pro spoléhající se stranu se zde dále stanoví, jakým způsobem má přistupovat k informacím o zneplatnění certifikátu, jak často se tato informace aktualizuje či pro jaké účely byl certifikát vydán. Nahlédneme-li do zákona o elektronickém podpisu, pak můžeme konstatovat, že Certifikační politika určí způsob plnění v něm stanovených povinností.

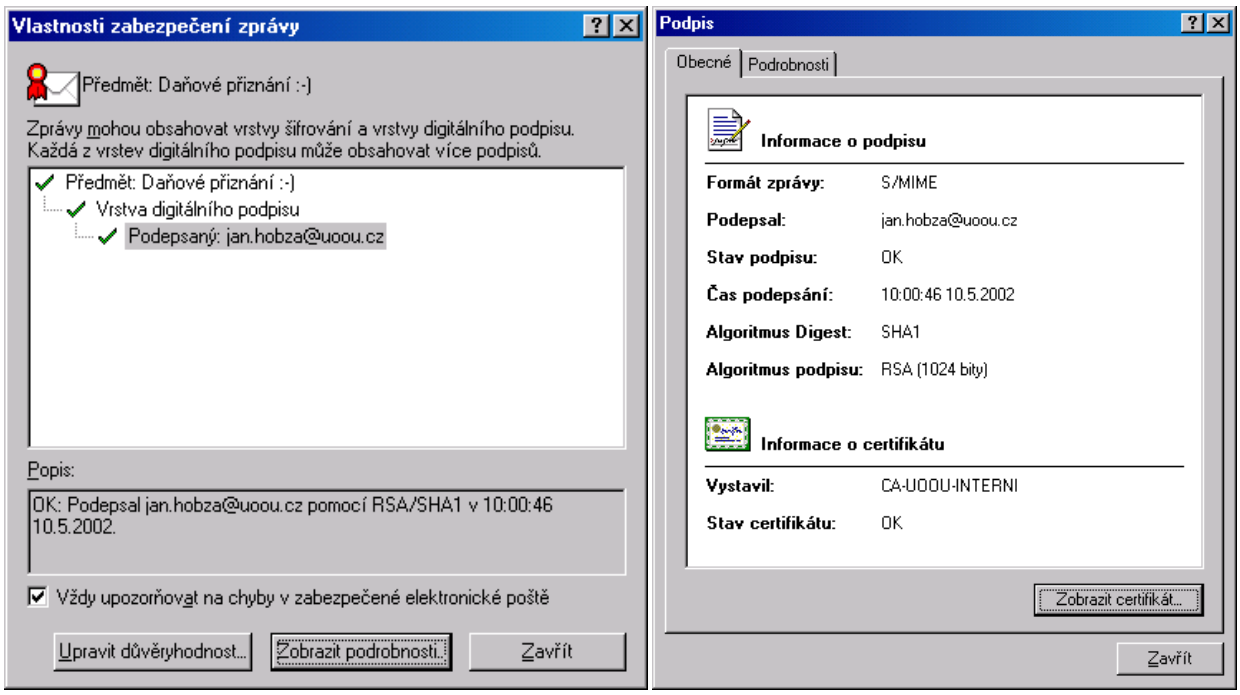
V ideálním případě by si podepisující osoba měla vybrat takového poskytovatele resp. takovou certifikační politiku, která vyhovuje jejím záměrům a splňuje i požadavky spoléhající

se strany. Vzhledem k velmi úzkému spektru těchto možností na současném trhu je tento ideální případ spíše fikcí či vizí budoucnosti. V každém případě však ještě před podepsání smlouvy doporučuji si danou Certifikační politiku důkladně přečíst a vzít na vědomí všechny povinnosti, které mi ukládá.

Země elektronického podpisu

Rok 1997 byl nejen dobrým ročníkem pro vinaře, ale i příznivou dobou pro elektronický podpis. V Německu, v Rakousku a v Itálii se narodily zákony o elektronickém podpisu. Každý postavený na trochu jiných principech a každý s trochu odlišnou působností, ale jedno měly společné. Na dobré úrovni definovaly požadavky na elektronický podpis a umožnily jeho používání pro jisté právní úkony. Právo tak zpětně reagovalo na požadavky praxe.

Po vydání Směrnice 1999/93ES bylo nutné i tyto zákony upravit. V průběhu jednoho až dvou let dokázaly všechny tři státy uvést své předpisy do souladu s touto směrnicí. Podobně reagovala i většina ostatních členských států, které přijaly své zákony o elektronických podpisech, ovšem naši tři pionýři měli jistou výhodu.



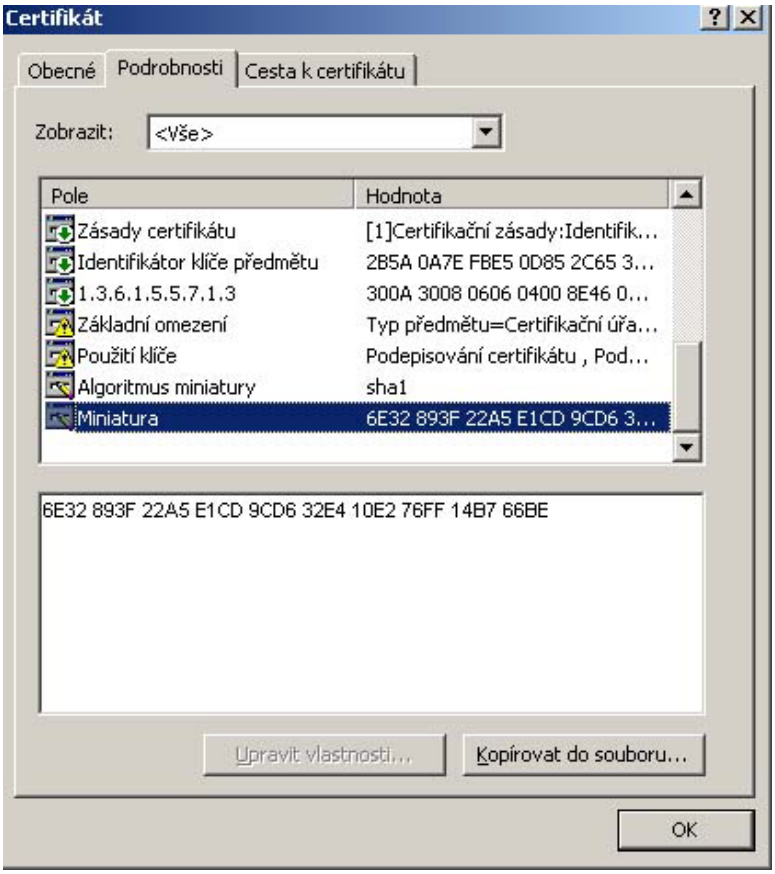
Implementace směrnice si mimo přijetí předpisů na úrovni zákonů vyžaduje i technickou standardizaci. To si uvědomovala i Evropská komise a tak zřídila odpovědné orgány, které tuto činnost mají realizovat (viz. č. 15/2002). Jak již ale víme, vytváření standardů je běh na dlouhou trať a tak vše je zatím ve fázi příprav. Důsledkem toho je, že řada členských států vyčkává s technickými požadavky a elektronický podpis je u nich stále ještě v plenkách. O mnoho jinak je tomu u našich „favoritů“.

V Německu právě před rokem vyšel upravený prováděcí předpis, který odkazuje na národní normy a standardy pro produkty elektronického podpisu. Samotná vyhláška je pak více méně technický předpis a plní funkci vzorové certifikační politiky. RegTP, což je orgán, který plní pro elektronické podpisy obdobnou funkci jako náš Úřad pro ochranu osobních údajů, do této chvíle akreditoval již 17 poskytovatelů certifikačních služeb a vyhodnotil

dlouhou řadu bezpečných produktů pro elektronické podpisy. Zkušenosti z praxe se promítly i do německé legislativy, která jde daleko za požadavky Směrnice. Příkladem může být zákonná úprava vytváření časových razítek (poskytují důkaz existence elektronických dat v čase) nebo atributové certifikáty ke kvalifikovaným certifikátům (je možné je použít jako autentizační prostředek v uzavřených systémech). Elektronický podpis je v Německu skutečnou alternativou.

Ověření certifikátu poskytovatele

V podmínkách pro udělení akreditace pro poskytování certifikačních služeb jako akreditovaný poskytovatel(§ 10 zákona č. 227/2000 Sb.) v odstavci 7 je uložena následující povinnost : „Součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem“.



V praxi to znamená, že akreditovaný poskytovatel certifikačních služeb předloží Úřadu všechny své kvalifikované certifikáty, které chce používat, a to ve všech formátech, které nabízí (zpravidla DER, TXT a PEM, případně EDI). Jedná se o kvalifikované certifikáty poskytovatele, které je nutné instalovat do uživatelských aplikací a které slouží k ověření podpisů kvalifikovaných certifikátů a CRL (seznamu kvalifikovaných certifikátů, které byly zneplatněny). V současné době provádí Úřad ověření certifikátů výpočtem otisků a jejich zveřejněním na různých distribučních místech. Běžně ve věstníku Úřadu, na jeho webových stránkách či v odborných časopisech (např. Crypto-World). Věstník Úřadu lze považovat za důvěryhodný zdroj, další zdroje mají pochopitelně spíše informativní povahu.

Pro uživatele má toto ověření zásadní důsledky. Díky němu je schopen ověřit, zda certifikát poskytovatele nebyl podvržen. Stačí v některém z viewerů (např. v produktech MS Outlook, MS Internet Explorer) otevřít certifikát, o němž chceme rozhodnout, zda je či není ověřen Úřadem. Zobrazí se nám následující (nebo jemu velice podobný – podle verze produktu) výsledek , který můžeme vidět na přiloženém obrázku.

V položce „miniatura“ pak najdeme otisk certifikátu. Použitá hašovací funkce je uvedena v položce „algoritmus miniatury“ (zpravidla SHA-1). Nyní stačí porovnat tento otisk s otiskem uvedeným ve Věstníku Úřadu, resp. s otiskem, který je zveřejněn na webové stránce

Úřadu. Pro otisk kvalifikovaného certifikátu První certifikační autority a.s. ve formátu DER je uvedena v těchto zdrojích hodnota: 6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE.

Porovnáním zjistíme, že tato hodnota je shodná s údajem v miniatuře – jedná se tedy o kvalifikovaný certifikát poskytovatele, který byl ověřen Úřadem. Na takovýto certifikát se můžete spolehnout a nic nebrání jeho instalaci.

Pro porovnání certifikátů v ostatních formátech potřebujete k výpočtu otisků použít některou z dostupných aplikací. Takto vypočtený výsledek opět jednoduše porovnáte s hodnotou otištěnou ve Věstníku. Úřad připravuje zveřejnění vhodné aplikace pro výpočet otisků certifikátů pomocí hašovacích funkcí SHA-1 a MD5 na své webové stránce.

Dovolená ve Francii

U jednotlivých států EU můžeme vysledovat odlišné způsoby promítnutí požadavků Směrnice 1999/93ES do právních řádů. Klasický model, který částečně odpovídá i českému přístupu, představuje Německo. Zde byl v roce 2001 přijat nový zákon o elektronickém podpisu a k němu i prováděcí vyhláška, která upřesňuje požadavky zákona. Dále byly novelizovány klíčové právní předpisy, jakými jsou občanský zákoník či zákon o sociálním pojištění. Druhý model reprezentuje Francie. Zde došlo k novelizaci hlavních právních předpisů na úrovni zákonů. U řady právních úkonů tak bylo umožněno, aby byly činěny v elektronické formě, jejíž náležitosti má později upravit prováděcí předpis. Větší váha se tedy klade na podzákonné právní předpisy, jejichž přijímání je více flexibilní. Podobnou cestou se vydala i Itálie.

Jak již bylo zmíněno, Francie přistoupila k implementaci Směrnice lehce odlišným způsobem. Francouzský parlament vydal 13. 3. 2000 zákon č. 2000-230, který pouze novelizuje občanský zákoník. Ve svých šesti článcích naplňuje požadavek článku 5 Směrnice, který upravuje právní důsledky elektronických podpisů. Dále odkazuje na prováděcí předpis Státní rady, který vešel v platnost 31. 3. 2001 a který konkretizuje jednotlivé požadavky na elektronický podpis. Tato vyhláška odpovídá svým obsahem nejlépe našemu zákonu o elektronickém podpisu a ukládá Certifikační komisy vlády dohled nad dodržováním povinností stanovených zákonem a souvisejícími předpisy. Certifikační komise má zároveň povinnost připravovat vyhlášky, které stanoví procesní a technické požadavky na poskytovatele certifikačních služeb.

Francie, podobně jako Česká republika, se rozhodla jít cestou zavádění elektronického podpisu ve státní správě. Certifikační komise za tímto účelem vydala zvláštní Certifikační politiku (http://www.minefi.gouv.fr/dematerialisation_icp/pc_type_minefi_dsi.pdf), která odpovídá požadavkům státní správy. Poskytovatelé certifikačních služeb, kteří chtějí působit v této oblasti, musí svoje služby realizovat v souladu s touto politikou. Pokud jejich služby odpovídají jejím požadavkům, mohou prohlásit své certifikáty za odpovídající. V současnosti existuje ve Francii 10 poskytovatelů, kteří vydávají tyto certifikáty. Jistou paralelu je možné spatřit i se současným stavem u nás. Po akreditaci prvního poskytovatele certifikačních služeb se vyskytly problémy s aplikací stávajících kvalifikovaných certifikátů ve státní správě, konkrétně v některých silových ministerstvech. Jednalo se o nedostatečnost povinných položek v kvalifikovaných certifikátech, jak je definuje zákon o elektronickém podpisu v § 12. Kamenem úrazu byla nejednoznačná identifikace tzv. Subjektu certifikátu, tedy držitele dat pro vytváření elektronického podpisu. Snaha o řešení vyústila v novelu zákona o elektronickém podpisu, která již byla vydána ve Sbírce zákonů. Je otázkou, jaké další

požadavky bude mít státní správa na certifikační služby a zda budou definovány v obdobném dokumentu jakým je francouzská Certifikační politika státní správy.

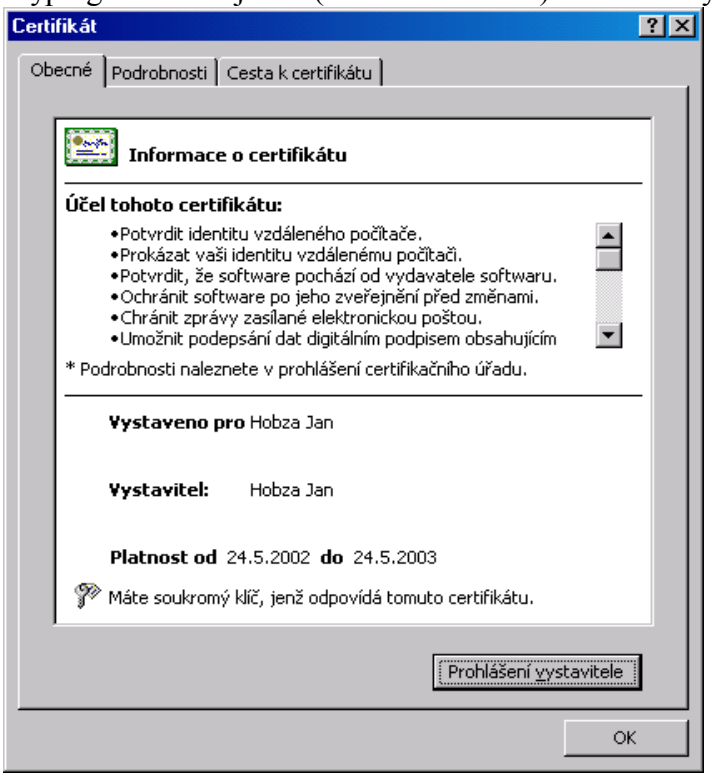
Intervat

V Belgii se pomalu a především jistě rozebíhá nový projekt ministerstva financí s názvem Intervat. Jedná se o nám velmi dobře známou elektronickou formu podávání daňových přiznání. To vše musí být ze zákona opatřeno elektronickým podpisem a kvalifikovaným certifikátem.

Belgické ministerstvo financí si za tímto účelem stanovilo podmínky a na jejich základě vybralo dva poskytovatele certifikačních služeb, kteří kvalifikované certifikáty pro účely Intervatu mohou vydávat. Jsou jimi Belgacom E-trust a Global Sign.

Plátce DPH, který chce využívat elektronickou formu podávání daňových přiznání, musí nejdříve uzavřít smlouvu s jedním z uvedených poskytovatelů. Její součástí je i příslušná Certifikační politika ale také Certifikační prováděcí směrnice (u většiny mně známých poskytovatelů se tento dokument považuje za neveřejný). Po přečtení a vlastnoručním ☺ podepsání smlouvy, zajde žadatel na registrační autoritu. Ta ověří jeho totožnost a správnost dokumentů a vydá mu certifikát. Tento postup již všichni známe.

Belgacom E-trust však poskytuje ještě jinou službu, o které jsme v našem seriálu zatím nepsali. Soukromý klíč k podepisování a veřejný klíč k ověřování podpisu si většinou žadatel generuje na svém počítači. Používá k tomu služeb svého poštovního klienta a jeho kryptografického jádra (CSP – viz díl 4). Jsou ale tyto služby bezpečné? Belgacom raději vytvořil program, který žadateli sám vygeneruje oba klíče, vytvoří za něj žádost o certifikát a zašle jí samostatně do registrační autority. Při generování klíčů používá jako náhodnou složku pohyb myši, kterou uživatel pohybuje po obrazovce. Tento malý program (zabalený má asi 2,4 MB) umožňuje dokonce vytvořit vlastní certifikát a podepsat jej vlastním soukromým klíčem. Jeho právní váha je samozřejmě minimální, přirovnatelná k váze testovacích certifikátů, které vydávají i naše certifikační autority. Jeho kouzlo však spočívá v tom, že jako vystavitel (tedy certifikační autorita) budete v certifikátu uvedeni Vy, tedy Vaše jméno, a jeho platnost je dokonce jeden rok.



„Vydejte si svůj vlastní certifikát“

Více informací o projektu Intervat můžete najít na této adrese: http://www.e-trust.be/intervat/intervat.html. Program, o kterém byla řeč, je dostupný na této adrese: http://www.e-trust.be/en/downloads/Belgacom%20E-Trust%20KeyGen-v2.7.1.zip.

Nové povinnosti správních orgánů

Parlament schválil, prezident podepsal a ve Sbírce zákonů 4. června vyšel neobjemný zákon č. 226/2002. Většina z nás by tuto strohou informaci přešla bez dalšího povšimnutí, kdyby onen zákon nenovelizoval náležitosti elektronických podání a s tím spojených úkonů. Novela se týká zákona o elektronickém podpisu, správního řádu, občanského soudního řádu, zákona o správě daní a poplatků a trestního řádu.

Novela zákona o elektronickém podpisu, kterou tento zákon provádí, je pouze kosmetická a nemá zásadní důsledky pro používání elektronických podpisů. Proto se v tomto článku omezím jen na změnu správního řádu, jelikož ta se dotkne většin z nás.

Správním orgánům se zde nově ukládá povinnost zveřejnit na své úřední desce nebo způsobem umožňujícím dálkový přístup (např. na internetovém serveru orgánu) následující informace:

a) Úřední hodiny, ve kterých je otevřena podatelna,
b) elektronickou adresu své podatelny,
c) formu technického nosiče pro doručování podání v elektronické podobě,
d) seznam kvalifikovaných certifikátů zaměstnanců nebo elektronické adresy, na nichž se nacházejí,
e) další možnosti učinit podání pomocí jiných elektronických přenosových technik.

Zákon č. 226/2002 Sb. nabude účinnosti dne 1. července 2002. To znamená, že od této chvíle budou mít občané právo uvedené informace vyžadovat a správní orgány budou mít povinnost je zveřejnit. Jelikož se dané údaje týkají elektronických podatelen, doporučuji při jejich obsahu (a tedy i při zřizování a konfiguraci elektronických podatelen) vycházet ze standardu ISVS č. 16/01.01 (http://www.uvis.cz/uvis/tisk.nsf/standardy?OpenView), který má stanovit požadavky na technické a programové vybavení podatelen.

Dále se § 19 správního řádu doplňuje o odstavec 6. Ten ukládá osobám, které činí podání v elektronické podobě, aby současně uváděly poskytovatele certifikačních služeb, který jim certifikát vydal, nebo aby certifikát přiložili k podání. Jaké jsou důsledky nedodržení této povinnosti však předpis již nestanoví.

Obsah zákona č. 226/2002 Sb. je zajímavý i z hlediska změny trestního řádu a především zákona o správě daní a poplatků. Jeho znění je možné najít na stránkách ministerstva vnitra (http://www.mvcr.cz/sbirka/2002/sb087-02.pdf).

Elektronické podatelny

Náš úřad často přijímá dotazy různých orgánů státní správy, jak se stavět k elektronicky podepsaným podáním, jak takové podpisy ověřovat a jak za tímto účelem vybavit své úřady. Na tyto otázky je možné najít odpovědi v nařízení vlády č. 304/2001 Sb.

(http://www.mvcr.cz/sbirka/2001/sb117-01.pdf) a v nově vydaném standardu ISVS 016/01.01 pro provoz elektronických podatelen (http://www.uvis.cz/uvis/tisk.nsf/pages/6636A9CBB4C09A09C1256BCA002C4805?OpenDocument). Níže uvedené povinnosti jsou pouze přejaty z těchto a dalších souvisejících.

Podle nařízení vlády, vydaného k provedení zákona o elektronickém podpisu, musí orgány veřejné moci zřídit jednu nebo více elektronických podatelen. Jejich úkolem je především přijímání a potvrzování přijetí podání a příprava na jejich následné zpracování. Podatelny, které zpracovávají podání podle zákona o správě daní a poplatků, musí též zajišťovat doručování písemností na e-mailovou adresu žadatele.

Součástí činností podatelny musí být především kontrola čitelnosti podání (tj. zda je zpráva v některém z akceptovatelných formátů – povinně .txt nebo .htm a volitelně další jako .rtf, .pdf, .doc apod.– a zda neobsahuje viry, červy, trojské koně apod.). Dále zda kvalifikovaný certifikát žadatele je platný a zda jej vydal akreditovaný poskytovatel. Pokud podání nebude mít tyto náležitosti, musí orgán veřejné moci postupovat podle předpisů upravujících odstraňování vad podání (podání má vady). Mezi další povinnosti podatelny patří archivace příchozí pošty podle zákona č. 97/1974 Sb., o archivnictví.

Elektronická adresa podatelny musí být ve formátu *posta@<doména_orgánu>.cz* podle standardu ISVS č. 002/01.03. Příjem a odesílání elektronických zpráv musí podporovat minimálně protokoly SMTP a POP3 a kódování zpráv ve formátu MIME a S/MIME. Ostatní technické a programové vybavení musí odpovídat standardům ISVS vydaným ve Věstníku ÚVIS.

Elektronická podatelna je informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb. Z toho vyplývá řada poměrně zásadních povinností. Pro zavádění a provoz podatelny je nutné zpracovat bezpečnostní projekt podle Standardu ISVS 005/01.01. Jeho součástí je definování požadavků na personální a fyzickou bezpečnost, režimové zabezpečení a bezpečnost IS. Technické vybavení podatelny musí mít atest na shodu s technickými požadavky Standardu ISVS 016/01.01. Atestaci ve smyslu zákona 365/2000 Sb., provádí několik komerčních subjektů, jejichž seznam je na adrese ÚVIS (http://www.uvis.cz/uvis/uvis.nsf/pages/atestace). O atest může žádat jak dodavatel systému, tak orgán veřejné moci, který podatelnu provozuje. Pokud orgány veřejné moci již provozují elektronickou podatelnu bez jejího atestu, musí jej zajistit a to z vlastních prostředků.

Atestace

Součástí povinností orgánů státní správy při zavádění a provozu elektronických podatelen je i získání atestu na technické vybavení podatelny. Tento atest se týká shody s technickými požadavky obsaženými v článku 4.5 Standardu ISVS 16/01.01 a jakosti dokumentace k technickému vybavení podatelny (systémové příručky, uživatelské příručky a školící texty v rozsahu a struktuře vyžadované Standardem ISVS pro náležitosti životního cyklu).

Podmínky shody se Standardem ISVS pro náležitosti životního cyklu budou dodavatelem produktu splněny, pokud k atestaci předloží dokumenty systémová příručka, uživatelská příručka a školící a učební texty. Dokument systémová příručka musí minimálně obsahovat popis systému podatelny, systémovou a programátorskou dokumentaci a zprávu o provedených testech. Uživatelská příručka obsahuje popis systému pro potřebu uživatelů,

návod k obsluze a provozní řád vymezující práva a povinnosti uživatelů. Součástí učebních textů může být i dokumentace zakoupená od dodavatele systému. Elektronická podatelna je informačním systémem veřejné správy, a proto musí být při jejím zavádění a provozu dodržovány standardy ISVS. To zahrnuje i vypracování Evidenčního listu pro projekt dodávky systému a Evidenční list pro uvedení do provozu podle Standardu 017/01.01, které je nutné zaslat na ÚVIS. Tyto dokumenty ovšem nejsou předmětem atestace podatelny.

Splnění technických podmínek článku 4.5 Standardu ISVS 16/01.01 se v atestačním řízení ověřuje s pomocí metodiky atestace jakosti s tím, že předmětem atestace je pouze funkčnost produktu. Ta se týká především těchto bodů:

- Zapisování doručení zpráv (automatizovaně) do archivu přijaté pošty a ukládání zpráv v souladu se zákonem č. 97/1974 Sb.
- Zapisování došlých podání do evidence (manuálně nebo automatizovaně)
- Kontrola na přítomnost virů, červů, trojských koňů apod.
- Ověřování podpisů a certifikátů odesílatele.

Řízení se zahajuje podáním žádosti o udělení atestu u některého z atestačních středisek. Součástí žádosti by měly být výše uvedené dokumenty a také prohlášení dodavatele, že zprávy elektronické podatelny jsou zpracovávány v souladu se zákonem č. 97/1974 Sb., o archivnictví. Po té následuje bližší komunikace žadatele a atestačního střediska a vlastní proces hodnocení a atestace. Atesty se vydávají na dobu 1 - 5 let, dle rozhodnutí příslušného pracovníka atestačního střediska. ISVS buď atest "splňuje", "splňuje s výhradami" nebo "nesplňuje". V posledních dvou případech vydá atestační středisko seznam nedostatků a povede se správcem připomínkové řízení, po odstranění nedostatků atestační středisko atest vydá. Po první atestaci se pouze provádí tzv. přírůstková atestace, která kontroluje pouze nové části ISVS (podatelny), které nebyly ještě atestovány a ty, kterým atestace vypršela.

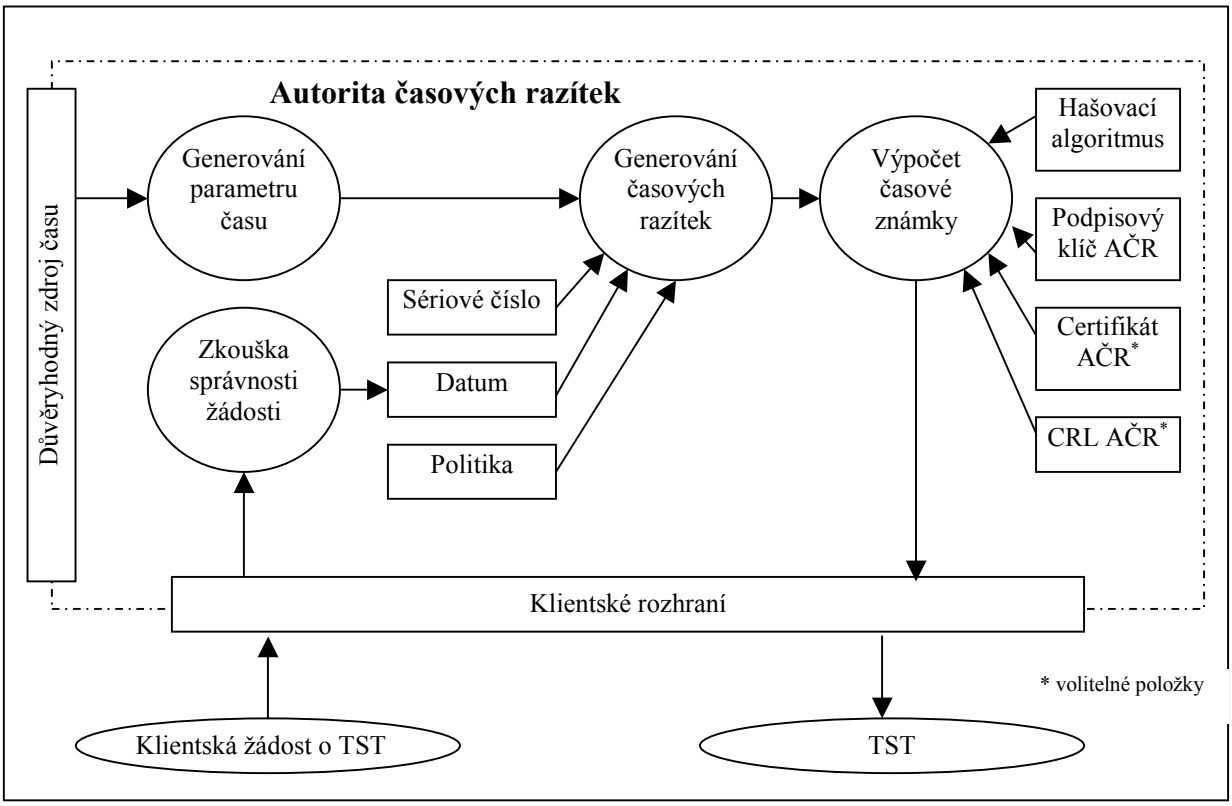
Autorita časových razítek

Pro ověření elektronického podpisu může být v určitých situacích potřebné ověřit i čas, ve kterém byl elektronický podpis vytvořen. Jedná se především o situace, kdy:

1. v průběhu doby platnosti certifikátu podepisující osoby mohlo dojít ke kompromitaci jejího soukromého klíče a ta jej z tohoto důvodu zneplatnila. V takovém případě je nutné zjistit, zda byl elektronický podpis vytvořen před okamžikem zneplatnění certifikátu. Nebo
2. certifikát podepisující osoby je omezen dobou své platnosti, která je vymezena v položkách certifikátu. Po jejím vypršení je certifikát již neplatný a není možné se na takový certifikát spolehnout. Nebo
3. právní předpisy mohou vyžadovat jako náležitost některých právních úkonů určení okamžiku, kdy byly učiněny. Pokud se takové právní úkony činí elektronicky je vhodné za účelem důvěryhodného určení času použít adekvátní elektronický nástroj.

Problémy spojené s důvěryhodným určením času v uvedených situacích je možné uspokojivě vyřešit dvěma způsoby. Jedním z nich je používání časových značek (time-mark). Jedná se o auditovatelné záznamy uchovávané v bezpečném prostředí třetí důvěryhodnou stranou, která spojuje zasílaná data s hodnotou času při jejich přijetí do archivu. Druhý způsob představuje časové razítko (time-stamp) resp. časový token (time-

stamp-token). Tato technologie je v poslední době velmi diskutovanou především díky rozvoji PKI pro certifikační autority. Jedná se o request/response komunikaci žadatele a poskytovatele služby časových razítek, který k zaslaným datům přidává časové razítko a vrací žadateli podepsaný časový token (viz. obrázek).



Obecně můžeme říci, že časové razítko poskytuje důkaz existence v čase, tedy důkaz, že daná data existovala před uvedeným časem. Časové razítko je tedy rozhodným nástrojem pro určování, zda elektronický dokument a tedy i elektronický podpis byl vytvořen v okamžiku platnosti jeho certifikátu. Proces vytváření časové razítka je patrný z obrázku. Žadatel (jakákoli osoba, která má zájem o získání časového razítka pro svoje data) nejdříve zašle AČR žádost o časové razítko. Její součástí jsou především předmětná data, resp. jejich otisk. Přesný formát žádosti specifikuje dokument RFC 3161. AČR po přijetí žádosti zkontroluje její správnost a postoupí ji do generátoru časových razítek. Zde se vytváří časové razítko jako datová položka, jejíž součástí je hodnota času, sériové číslo razítka, identifikátor politiky AČR a datum. Časové razítko se pak připojí k zaslanému otisku a tato dvojice se podepíše soukromím klíčem AČR. Tím vznikl tzv. časový token, který se zasílá žadateli běžně ve formátu ASN.1 .der či .pem.

Státní sociální podpora s elektronickým podpisem

Ministerstvo práce a sociálních věcí vykročilo do měsíce července rázným elektronickým krokem. Na jeho serveru forms.mpsv.cz se od 1.7.2002 rozeběhly první aplikace, které umožňují žadatelům o sociální dávky elektronicky podepisovat a odesílat vyplněné formulářové žádosti.

Jako jeden z prvních orgánů státní správy zprovoznilo Ministerstvo práce a sociálních věcí takto komplexní projekt elektronických služeb občanům. Na výše uvedených stránkách

je možné najít elektronické formuláře pro dávky sociální podpory, které je možné ihned vyplnit. Formuláře jsou součástí aplikace, která zároveň kontroluje integritu vyplňovaných údajů. K lepšímu uživatelskému pohodlí slouží návod na vyplňování a obecné informace o nárocích na sociální dávky.

Po vyplnění formuláře je možné jej vytisknout a fyzicky odnést na příslušný úřad spolu s dalšími náležitostmi (různá ověření, potvrzení apod.). Jejich povinný seznam vám aplikace automaticky vypíše na obrazovku. Je zde ovšem možnost vyplněnou žádost elektronicky podepsat a zaslat ji po internetu. K tomu je třeba mít nainstalovaný kvalifikovaný certifikát s jednoznačným bezvýznamovým identifikátorem od I.CA. První certifikační autorita vám takový certifikát vydá na základě žádosti přímo na jednom z jejích registračních míst. Při žádosti o certifikát provede certifikační autorita dotaz na MPSV, které obratem vyhledá a zašle onen identifikátor zpět do centrály I.CA. Generování certifikátu tedy netrvá o mnoho déle.

K úspěšnému podepsání a odeslání žádosti ještě potřebujete mít na svém počítači systémovou komponentu OKSign.ocx. Její stáhnutí a spuštění se provede automaticky při volbě „podepsat“; musíte mít ovšem povoleno stahovat a spouštět prvky ActiveX. Komponenta OKSign je podepsána certifikační autoritou MPSV. Tím je zajištěna její integrita a autentičnost. Při jejím stahování by se mělo objevit upozornění spolu s odkazem na certifikát podpisu (viz obrázek).

Server forms.mpsv.cz je také vybaven vlastním certifikátem, který vám umožní šifrování dat při jejich odesílání (pomocí protokolu SSL). Pouze při prvním přihlášení na

stránky je nutné jej nainstalovat do úložiště certifikátů na vašem PC. Z pohledu ochrany dat občanů se tedy celková aplikace zdá být kvalitní a nastiňuje cestu pro další orgány státní správy. Jediným možným otazníkem jsou přílohy žádostí, které je stejně nutné pořizovat a zasílat úřadu v papírové formě, což může řadu potenciálních uživatelů odrazovat.

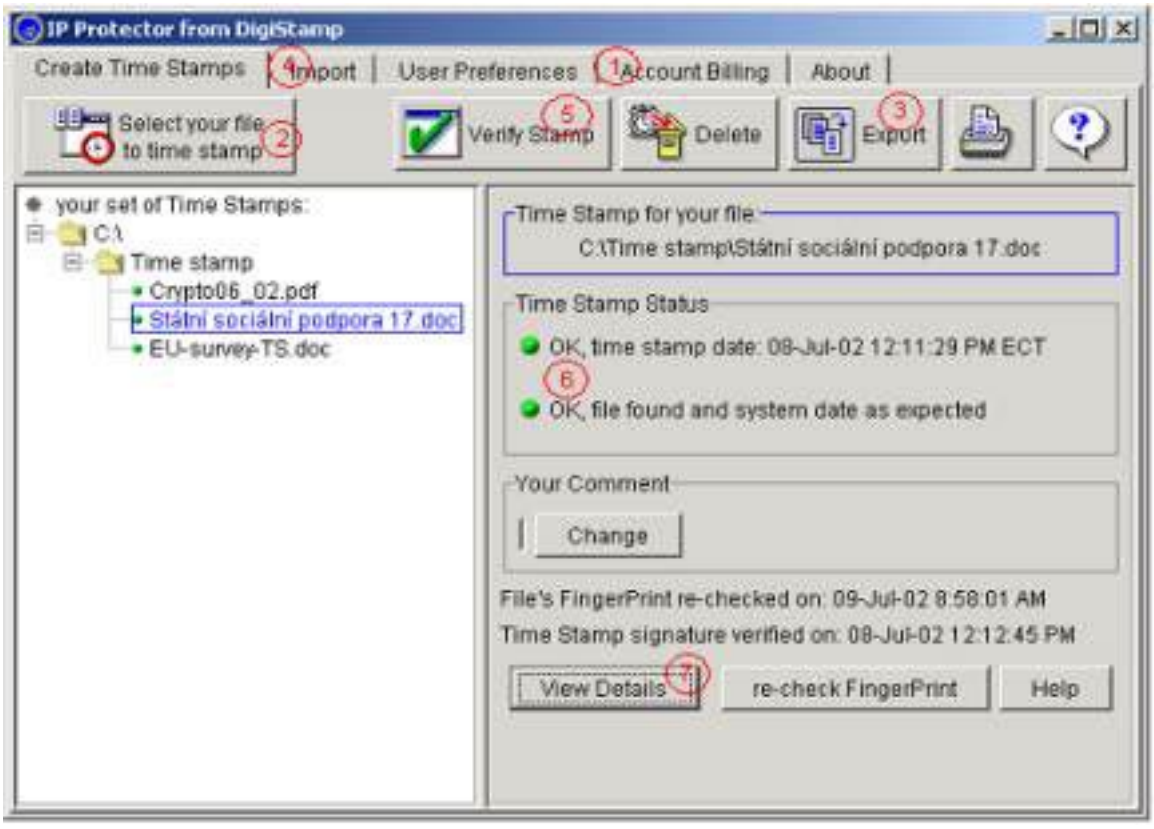
Vytváření časových razítek

V předminulém dílu jsme se věnovali autoritě časových razítek a jejich významu. Dnes si služby jedné z nich i vyzkoušíme.

Jednou z mála autorit, která nabízí své služby zdarma (alespoň po určitou dobu), je americký server www.e-timestamp.com. Na internetu je možné najít i další autority poskytující podobné služby zdarma, ale většinou se jedná o služby časových značek (viz předminulý díl) nebo je jejich infrastruktura příliš vzdálena novým normám, které se v současné době v Evropě prosazují (RFC 2459, 2630, 3161, ETSI TS 101861 a jiné).

Pro začátek je nutné si zřídit anonymní účet na adrese http://www.e-timestamp.com/AcctSetup1.htm. Pro naše testovací účely vám bude k registraci stačit pouze vaše emailová adresa a zvolené heslo. Dále je třeba si stáhnout instalační balíček z adresy http://www.e-timestamp.com/options.htm. Tento balíček obsahuje klientský program „IP PROTECTOR“ pro komunikaci s autoritou časových razítek (AČR) a správu časových razítek. Po jeho instalaci je nutné vyplnit v záložce Account billing (viz č. 1 na obrázku) číslo vašeho účtu a vaše heslo. Další ovládání je již velice intuitivní.

Nejdříve si vyberete soubor, pro který chcete získat časové razítko (č. 2). Může jím být jakýkoli textový, obrázkový, či spustitelný soubor, ale také elektronicky podepsaná emailová zpráva a podobně. Je ovšem doporučené, aby tento soubor byl alespoň minimálně chráněný proti změnám a byl uložen ve zvláštním adresáři. Po vybrání souboru se aplikace dotáže, zda opravdu chcete tento soubor „orazítkovat“. Poté se z jeho obsahu vypočítá haš a odešle se do časové autority. Ta za okamžik vrátí časový token s časovým razítkem, podpisem a původním hašem dokumentu. Časové tokeny se ukládají do souborů IPPDB2 v domovském adresáři aplikace. Je však možné je exportovat (č. 3) a zaslat je spolu s původním souborem druhé osobě.



Druhá strana po přijetí obou souborů nejdříve provede jejich import od aplikace IP PROTECT (č. 4) a poté spustí ověření časového razítka (č. 5). Aplikace v tento okamžik spočítá nový haš z importovaného dokumentu a porovná jej s hašem v časovém tokenu. Poté ještě ověří platnost časového razítka pomocí jeho podpisového certifikátu a vrátí uživateli zprávu (č. 6). Je ještě možné zobrazit podrobnosti o časovém razítku (hašovací funkce, sériové číslo apod.) nebo jej vytisknout v grafickém provedení (č. 7).

Bohužel dosud není mnoho autorit časových razítek, které by nabízely své služby široké veřejnosti. Je třeba si ale uvědomit, že základní normy pro jejich provoz teprve vznikají a ani legislativa v EU jim zatím nepřikládá odpovídající váhu. Časová razítka mají díky svým vlastnostem budoucnost jistou a jistě se nimi v dohledné době setkáme.

Elektronické podatelny č. 2

Dnes se vrátíme k tématu, které jsme probírali již před několika týdny, a to k elektronickým podatelnám a atestacím. Vzhledem k vašemu ohlasu na tyto dva články se dnes pokusím nastínit způsob, jakým mohou příslušné státní orgány naplnit požadavek na zřízení elektronických podatelen vyplývající z nařízení vlády č. 304/2001 Sb.

Úřad pro veřejné informační systémy vydal v červnu tohoto roku Standard ISVS č. 016/01.01, který se zabývá provozem a atestací elektronických podatelen. Již víme, že elektronická podatelna je podle tohoto standardu informačním systémem veřejné správy. Pro prokázání shody elektronické podatelny s tímto standardem se ovšem nevyžaduje atest elektronické podatelny. Ten je vyžadován pouze na technické vybavení podatelny a související dokumentaci. Technické vybavení elektronické podatelny musí splňovat požadavky článku 4.5 Standardu ISVS č. 016/01.01. Jedná se především o požadavky na funkčnost - ukládání přijatých zpráv, ověřování elektronických podpisů, formáty a kódování zpráv apod. Standard doporučuje, aby atest byl prováděn i s ohledem na bezpečnost, bezporuchovost a použitelnost vybavení.

Orgán veřejné moci může při akvizici elektronické podatelny postupovat v zásadě dvěma způsoby. Je možné pořídit vybavení, které již úspěšně prošlo atestačním řízením, nebo zažádat a projít procesem atestace na vlastní náklady (cena atestačního řízení se u většiny atestačních středisek pohybuje nad hranicí 10.000,- Kč). V obou případech bude ovšem nutné vlastními silami zpracovat bezpečnostní projekt elektronické podatelny a Evidenční listy pro akvizici vybavení a jeho uvedení do provozu (tyto listy se poté zasílají na ÚVIS).

Pokud se daný orgán veřejné moci rozhodne pro druhé řešení, tedy zakoupení technického a programového vybavení elektronické podatelny, které ještě nezískalo atest, či pokud již takto vybavenou podatelnu provozuje, bude nutné ještě zpracovat (či jinak získat) systémovou a uživatelskou příručku a školící a učební texty ve struktuře a rozsahu podle Standardu ISVS 005/01.01 (viz také předchozí díly seriálu). Pokud tedy i váš úřad půjde touto cestou, doporučuji nejdříve kontaktovat jedno z atestačních středisek a požádat o předběžnou konzultaci k vašemu vybavení a možnému řešení vaší podatelny. Tyto konzultace jsou u některých středisek bezplatné.

Elektronický podpis na Slovensku

V březnu tohoto roku přijala slovenská Národní rada zákon o elektronickém podpisu. Jeho cílem, stejně jako v případě českého zákona a nově přijímaných zákonů v členských státech EU, byla především harmonizace právního řádu s požadavky Směrnice 1999/93/ES o elektronických podpisech. Bylo tedy možné předpokládat, že slovenský zákon bude velmi podobný svým evropským předchůdcům. Zákon se však od ostatních liší již ve svém paradigmatu. V tomto krátkém článku se zaměříme jen na některé body, které odlišují slovenský zákon především od českého zákona o elektronickém podpisu. Podrobnější rozbor je možné najít v časopise Crypto-World č. 78/2002 (http://www.mujweb.cz/veda/gcucmp/).

První odlišnost můžeme spatřit hned v subjektivní působnosti slovenského zákona. Zatímco český zákon upravuje především práva a povinnosti subjektů při vydávání, používání a správě **kvalifikovaných** certifikátů (tedy akreditovaných poskytovatelů, poskytovatelů podle § 6 českého zákona a podepisující a spoléhající se strany, když odhlédneme od pravomocí Úřadu), slovenský zákon vymezuje svou subjektivní působnost negativně. Tj. upravuje práva a povinnosti při vydávání všech certifikátů pro elektronické podpisy, kromě certifikačních služeb v uzavřených systémech a kromě používání elektronického podpisu v rámci zákona o utajovaných skutečnostech. Důsledkem toho je, že veškeré certifikační autority (tedy i neakreditované), které vydávají na Slovensku certifikáty pro veřejnost, musí splňovat podmínky slovenského zákona o elektronickém podpisu.

Další odlišnost tkví v definici typů elektronických podpisů. Český zákon nepodmiňuje vznik zaručeného elektronického podpisu existencí odpovídajícího kvalifikovaného certifikátu ani dalšími náležitostmi. Slovenský zákon definuje zaručený elektronický podpis jako elektronický podpis vytvořený na základě kvalifikovaného certifikátu od akreditovaného poskytovatele pomocí bezpečného prostředku pro vytváření elektronických podpisů. Pouze takový podpis bude podle § 5 odst. 1 možné používat ve styku s veřejnou mocí. Důvěra v takovou komunikaci se přirozeně zvyšuje, ovšem použití bezpečných prostředků ji může značně prodražit. Další otázkou je, jakým způsobem bude možné dokázat, zda určitý zaručený podpis byl vytvořen pomocí takového prostředku.

Slovenský zákon pověřil Národní bezpečnostní úřad kontrolou nad poskytovateli certifikačních služeb a zmocnil jej k vydání řady prováděcích vyhlášek, které mají upřesnit některá jeho ustanovení. Na rozdíl od českého zákona, který dal našemu úřadu zmocnění k upřesnění pouze §§ 6 a 17 zákona (tedy povinnosti poskytovatelů a náležitosti prostředků pro elektronický podpis), pokrývá zmocnění slovenského zákona poměrně širokou oblast. Prováděcí vyhlášky mají upravit způsob vytváření podpisů a časových razítek, náležitosti kvalifikovaného certifikátu, požadavky na produkty elektronického podpisu atd. NBÚ opravdu neotálel a vyhlášky jsou v tuto dobu již platné, vydané ve sbírce zákonů.

Vyhlášky zavádějí čtyři formy zaručeného elektronického podpisu, přičemž jeho tři vyšší verze jsou spojeny s časovým razítkem. Z pohledu práva je určení okamžiku uzavření smlouvy či jiného právního úkonu zásadní otázkou. Jak víme, časové razítko je důvěryhodným nástrojem pro určení času, a tak je jeho legalizace jistým přínosem při vytváření důvěry v elektronický podpis.

Národní bezpečnostní úřad bude též provádět hodnocení bezpečných produktů pro elektronický podpis, tedy nástrojů, které budou používat certifikační autority, ale také podepisující osoby. To je úkol nelehký a náročný jak na čas, tak na peníze. Česká vyhláška

tento problém řeší také, ale vzhledem k chybějícím testovacím laboratořím je nutné zatím využívat služeb zahraničních hodnotitelů.

Rozdílné je též postavení slovenského NBÚ v certifikační cestě kvalifikovaných certifikátů. NBÚ má za úkol vytvořit kořenovou certifikační autoritu, která bude vydávat certifikáty akreditovaným poskytovatelům. Bude tedy vrcholem důvěry slovenského akreditačního schématu.

Akreditované certifikační autority mohou podle slovenského zákona také důvěru „dědit“ od jiných akreditovaných poskytovatelů formou křížových certifikátů. Zákon tak kombinuje dvě koncepce PKI (kořenovou CA a křížové certifikáty) k zajištění větší flexibility akreditovaných poskytovatelů.

Perspektivy jsou na Slovensku tedy slibné, doufejme, že se vyplní.

Odbor elektronického podpisu
e-mail: **Jan.Hobza@uoou.cz**
http://www.volny.cz/honzahobza

C. Mikulášská kryptobesídka

2. – 3. prosinec 2002, Praha

ECOM-MONITOR.COM

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop zaměřený na podporu úzké spolupráce odborníků pracujících na poli aplikované kryptografie a v příbuzných oblastech bezpečnosti, se koná za účelem podpory výměny informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez zbytečných problémů a starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop navazuje na úspěšná setkání Velikonoční kryptologie 3.-4.4.2002 v Brně a Mikulášskou kryptobesídku, která se konala 10.-11.12.2001 v Praze. Workshop se skládá z (a) neformálního setkání (a případně panelové diskuse) v pondělí *2. prosince 2002* a (b) prezentací příspěvků a diskusí v úterý *3. prosince 2002*.

Na workshopu budou předneseny dva zvané příspěvky:

Vincent Rijmen (Cryptomathic, Belgie) o kryptoalgoritmech Rijndael/AES a jeho úpravě Anubis,

Geraint Price (Royal Holloway a PricewaterhouseCoopers, UK) o možnostech PKI.

Pokyny pro autory

Zájemci mohou poslat své příspěvky zaměřené především na oblast aplikované kryptografie, ale i bezpečnostních aplikací kryptografie a dalších oblastí kryptografie. Šablony (Word a LaTeX) pro přípravu příspěvků lze stáhnout ze stránky
http://www.ecom-monitor.com/kryptobesidka/cfp.html .

Návrhy příspěvků (5-15 stran A4) bez uvedení informací o autorech a zjevných odkazů, s oddělenou stranou textu s autorovou emailovou adresou, telefonním číslem a poštovní adresou, musí programový výbor (PV) obdržet na níže uvedené adrese nejpozději do ***21. října 2002*.** Elektronická podání jsou preferována; papírová podání musí obsahovat 7 vytištěných kopií.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *5.listopadu*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), před ***21. listopadem***. Příspěvky mohou být napsány v češtině, slovenštině nebo angličtině.

Rozšířené abstrakty i kompletní příspěvky by měly být odeslány v RTF, HTML nebo ASCII.

Zasílání příspěvků

Preferujeme elektronické podání příspěvků.
E-mail: *Vaclav.Matyas@ecom-monitor.com*
Předmět: "MKB 2002"
Poštovní adresa: ***V. Matyáš***
ecom-monitor.com, a.s.
PO Box 7
664 01 Bílovice nad Svitavou

Důležitá data

Podání návrhů příspěvků:	21. října 2002
Oznámení o přijetí/odmítnutí:	5. listopadu 2002
Pracovní verze příspěvků:	21.listopadu 2002
Workshop:	2. – 3. prosince 2002
Podání finálních příspěvků:	11. ledna 2003

Programový výbor

Tonda Beneš, SAP ČR a UK Praha
Petr Hanáček, VUT Brno
Vašek Matyáš, ecom-monitor.com a MU Brno
Daniel Olejár, UK Bratislava
Tomáš Rosa, ICZ a ČVUT Praha
Pavel Vondruška, ČESKÝ TELECOM a.s.
Jozef Vyskoč, VaF Bratislava

Organizační výbor

Dan Cvrček, VUT Brno
Jaroslav Dočkal, Vojenská akademie Brno
Magda Procházková, ecom-monitor.com
Zdeněk Říha, ecom-monitor.com a MU Brno
Jan Staudek, MU Brno
Eva Špatná, ecom-monitor.com – tajemnice
Petr Švéda, MU Brno

D. Letem šifrovým světem

Informace

Na domovské stránce Crypto-Worldu v sekci „Přehled vybraných zdrojů – Slovensko“ jsem zařadil nový odkaz, který obsahuje velice hodnotné materiály z oblasti kryptologie:
http://www.kemt.fei.tuke.sk/predmety/KEMT414_AK/_materialy/
Stránka vzniká pod odborným dohledem doktora Drutarovského.
Milos DRUTAROVSKY
Technical University of Kosice
Department of Electronics and Multimedia Communications
Park Komenskeho 13
041 20 Kosice , Slovakia

O čem jsme psali v září v letech 1999 - 2001

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm
Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

E. 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 neprochází jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :
http://www.mujweb.cz/veda/gcucmp

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@ct.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . 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@ct.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení - !!!! POZOR ZMĚNA !!!!

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@ct.cz
vondruska.p@seznam.cz
pavel.vondruska@post.cz