Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 3/2002 **18. březen 2002**

3/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>350 e-mail výtisků)

Obsah : **Str.**

A. Vysvětlení základních pojmů zákona o elektronickém podpisu
Dagmar Bosáková, Pavel Vondruška

Seznam některých základních pojmů

Akreditace

Viz též **Poskytovatel certifikačních služeb**

Akreditace ve smyslu zákona o elektronickém podpisu je osvědčení vydávané Úřadem pro ochranu osobních údajů (dále jen Úřad) poskytovatelům certifikačních služeb. Požádat o udělení akreditace pro výkon činnosti akreditovaného poskytovatele může každý poskytovatel. V žádosti o akreditaci musí doložit skutečnosti podle § 10 odst. 2 zákona. Akreditovaný poskytovatel musí mít sídlo na území České republiky. Kromě činností uvedených v zákonu o elektronickém podpisu může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec. Nad činností akreditovaných poskytovatelů vykonává Úřad dozor.

Působení akreditovaných poskytovatelů je nezbytné v oblasti orgánů veřejné moci, neboť podle § 11 zákona: *V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.*

§ 2 písm. p) zákona: akreditací (se rozumí) osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb

Certificate revocation list (CRL)

Viz též **Seznam kvalifikovaných certifikátů, které byly zneplatněny**

Při vydávání certifikátu je stanoveno, a přímo v certifikátu uvedeno, na jaké časové údobí se vydává, resp. do jakého data bude platný. Mohou však nastat okolnosti, kdy je nezbytné ukončit platnost certifikátu dříve, než bylo při jeho vydání stanoveno. Může se jednat o změnu jména osoby, které byl certifikát vydán, nebo obecně o změnu některého z údajů uvedených v certifikátu, vyzrazení nebo hrozbu vyzrazení dat pro vytváření elektronického podpisu. Za těchto okolností poskytovatel ukončí platnost certifikátu. Poskytovatel vydává strukturovaný dokument, s předem stanovenou periodicitou vydávání, který se nazývá certificate revocation list (CRL – viz Certificate revocation list). CRL obsahuje přesný časový údaj, kdy byl vydán a identifikuje certifikáty, které byly zneplatněny. CRL je podepsán elektronickým podpisem poskytovatele a je veřejně přístupný, zpravidla na webových stránkách poskytovatele. Každý zneplatněný certifikát je v CRL identifikován svým unikátním číslem (jedinečným u daného poskytovatele). Toto číslo je certifikátu přiděleno už při jeho vydání. Osoba, která se na podpis spoléhá, do CRL nahlíží, aby zjistila, zda v něm není uvedeno číslo certifikátu, jehož platnost právě ověřuje.

Kdy osoba spoléhající se na podpis CRL zpravidla používá? Při přijetí elektronicky podepsané zprávy nejprve aplikace zkontroluje platnost certifikátu podepisující osoby, a to z hlediska doby jeho platnosti (zda neuplynula doba platnosti, která je v něm uvedena), a z hlediska toho, zda nebyl tento certifikát změněn - toto zjistí ověřením elektronického podpisu poskytovatele. Osoba spoléhající se na podpis se musí následně ujistit, zda platnost certifikátu nebyla ukončena předčasně (zpravidla nevykoná aplikace sama). Osoba spoléhající se na podpis "nahlédne" do CRL, který zveřejnil poskytovatel, který podepisující osobě certifikát vydal. Není ovšem nezbytné prohlížet jednotlivé položky CRL, ale lze jej "stáhnout" do svého počítače a implementovat do aplikace, která v rámci ověření zjišťuje, zda certifikát není v CRL uveden. Osoba spoléhající se na podpis by měla CRL pravidelně aktualizovat ("stahovat" aktuální CRL), neboť starší aplikace toto zpravidla sama neučiní, ani nerozpozná, že CRL není aktuální.

Zákon o elektronickém podpisu používá pojem „seznam certifikátů, které byly zneplatněny“. Vztahují se k němu zejména tato ustanovení:

§ 5 odst. 2 zákona: Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

§ 6 odst. 1 zákona (poskytovatel vydávající kvalifikované certifikáty je povinen)
písm. g): zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem
písm. h): zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát vydán nebo zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám

§ 15 odst. 2 zákona: Seznam certifikátů podle § 6 odst. 1 písm. g) musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn. Zneplatněné certifikáty není povoleno opětovně zprovoznit a používat.

Certifikační autorita

Viz též **Poskytovatel certifikačních služeb**

Poskytovatel certifikačních služeb je autorita, která je důvěryhodná pro uživatele certifikačních služeb, tj. je důvěryhodná jak pro podepisující osoby, kterým vydává certifikáty, tak pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty, za stanovených podmínek je zneplatňuje a vydává CRL (viz Certificate Revocation List). Vydané certifikáty a CRL podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci a je identifikovatelná jako subjekt, který je vydal.

Certifikační autorita může některé činnosti zajišťovat prostřednictvím jiných subjektů, např. služby registračních autorit (viz Registrační autorita), vždy však na ní zůstává odpovědnost za poskytované služby. Certifikační autorita může prostřednictvím jiných subjektů zajišťovat i vydávání certifikátů, vždy však data pro vytváření elektronického podpisu (soukromý klíč), kterým jsou tyto certifikáty podepisovány, musí být identifikovatelná jako náležející certifikační autoritě a certifikační autorita je odpovědná za náležité zacházení s nimi.

Certifikační autoritou se rozumí „certification-service-provider“ ve smyslu Směrnice 1999/93/ES o zásadách společenství pro elektronické podpisy a „poskytovatel certifikačních služeb“ ve smyslu zákona o elektronickém podpisu (viz Poskytovatel certifikačních služeb). Někdy je pod pojmem „certifikační autorita“ chápán pouze HW a SW, s jehož pomocí jsou certifikáty vydávány.

Certifikační politika

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen vydat certifikační politiku a umožnit k ní trvalý dálkový přístup. Tento dokument je z hlediska jeho zákazníků – tedy žadatelů o certifikát – velice důležitý. Obsahuje informace o poskytovateli, o jeho službách a jejich cenách. Na základě tohoto dokumentu může žadatel posoudit kvalitu nabízených služeb, dále například zjistit, zda je poskytovatel pojištěn nebo jak postupuje v krizových situacích. Certifikační politika slouží pro výběr vhodného poskytovatele. Doporučená struktura tohoto dokumentu je obsažena v RFC 2527.
K předepsanému obsahu certifikační politiky se vztahuje § 2 odst. 2 vyhlášky č. 366/2001 Sb.,

Obsahem certifikační politiky je zejména
stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy, a
popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

Certifikát

Viz též Kvalifikovaný certifikát

Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby. Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních

služeb a která spojuje data pro ověřování podpisu (viz Data pro vytváření a data pro ověřování elektronického podpisu) s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují.
Vydáním certifikátu poskytovatel stvrzuje, že data pro ověřování elektronického podpisu patřící určité osobě a že ve spojení s daty pro vytváření elektronického podpisu podepisující osoby, vykonávají požadované funkce.
Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby (ve smyslu: "tato data patří osobě X.Y."). Identitu podepisující osoby podle typu certifikátu může poskytovatel zjišťovat různými způsoby, v některých případech postačí e-mailová adresa, v jiných je nutné osobně prokázat totožnost příslušnými doklady.
Zákon o elektronickém podpisu neupravuje jiné předávání dat pro ověřování elektronického podpisu, než prostřednictvím kvalifikovaných certifikátů (viz Kvalifikovaný certifikát). V praxi jsou používány i jiné způsoby nebo certifikáty, které nejsou kvalifikované ve smyslu zákona o elektronickém podpisu. Certifikáty jako standardní způsob předávání dat pro ověřování elektronického podpisu používá například Microsoft Outlook nebo Outlook Express. Data pro ověřování elektronického podpisu lze také vystavit v internetové síti veřejných klíčů (např. u PGP) či na jakémkoliv jiném vhodném místě, kde se s nimi mohou seznámit ti, se kterými má podepisující osoba v úmyslu komunikovat. Pro ověření „pravosti“ dat pro vytváření elektronického podpisu se používá rovněž jejich podepisování jinou osobou, osobní předání jejich otisku (jednoznačné identifikace, angl. hash) například na vizitce nebo zaslání otisku e-mailem a následným ověřením telefonicky, pokud má ověřující jistotu, že danou osobu pozná po hlase.
V souvislosti s vydáváním certifikátů se lze setkat s pojmy „rekey“, „renewal“ a „update“. Ty souvisejí s vydáním nového certifikátu osobě, která má dosud platný certifikát vydaný tímto poskytovatelem. V této souvislosti mohou nastat následující situace, případně jejich modifikace:
-Nový certifikát je ve srovnání s dosud platným certifikátem vydán s jinými daty pro ověřování podpisu podepisující osoba, s jiným unikátním číslem a případně s uvedením jiné doby platnosti. Další údaje zůstávají nezměněny. Dosud platný certifikát může zůstat dále v platnosti, a to až do uplynutí doby platnosti v certifikátu uvedené, je však nepřípustné v tomto certifikátu jakékoliv údaje dále měnit, a to včetně dat pro ověřování podpisu podepisující osoby a doby platnosti certifikátu (zpravidla angl. rekey).
-Vydáním nového certifikátu je prodloužena platnost dat uvedených v dosud platném certifikátu. V novém certifikátu se ve srovnání s dosud platným certifikátem mění pouze doba platnosti a unikátní číslo. Další údaje, včetně dat pro ověřování podpisu podepisující osoby, zůstávají v novém certifikátu stejné jako v dosud platném certifikátu. (zpravidla angl. renewal.
-Nový certifikát je vydán z důvodu, že došlo k tak zásadním změnám v údajích uvedených v dosud platném certifikátu, že je nutné tento certifikát zrušit (zpravidla angl. update)

Zákon o elektronickém podpisu neobsahuje odpovídající pojmy pro rekey, renewal a up-date, ani speciálně neupravuje výše uvedené situace.

Vydávání a následné správě kvalifikovaných certifikátů se vztahuje celá ustanovení zákona o elektronickém podpisu, uveďme alespoň následující:
§ 2 písm. g) zákona: certifikátem (se rozumí) datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost

§ 6 odst. 1 zákona: (Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen)

písm. a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti kvalifikovaných certifikátů stanovené tímto zákonem
písm. b) zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné
písm. c) před vydáním kvalifikovaného certifikátu bezpečně ověřit odpovídajícími prostředky totožnost osoby, které kvalifikovaný certifikát vydává, případně i její zvláštní znaky, vyžaduje-li to účel kvalifikovaného certifikátu
písm. d) zjistit, zda v okamžiku vydání kvalifikovaného certifikátu měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát,
písm. f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat.

CRL viz **Certification revocation list**

Časové razítko

Časové razítko je údaj, který lze přidat k elektronicky podepsané datové zprávě a který stvrzuje, že datová zpráva existovala dříve, než k ní bylo toto razítko přidáno. Takové stvrzení musí učinit někdo důvěryhodný a nezávislý na podepisující osobě a příjemci zprávy. Může se jednat o jednu ze služeb, které poskytuje poskytovatel, nebo ji může nabízet jiný subjekt.

U datových zpráv, u kterých se předpokládá dlouhodobé uchování, je možné např. díky použití časového razítka prokázat, že datová zpráva byla podepsána v době platnosti příslušného certifikátu.

Vzhledem k tomu, že jiný způsob prokázání času, kdy byla datová zpráva elektronicky podepsána, je velmi problematický, je možné předpokládat rozvoj služeb časových razítek. Zákon o elektronickém podpisu používání časových razítek neupravuje.

Data pro vytváření a data pro ověřování elektronického podpisu

Viz též **Podepisující osoba, Digitální podpis**

Data pro vytváření elektronického podpisu slouží, jak název napovídá, pro jeho vytvoření. Nestačí však zprávu elektronicky podepsat, je ještě nutné zajistit, aby mohlo být ověřeno, kdo zprávu podepsal. K tomu slouží data pro ověřování elektronického podpisu, která musí být odpovídající datům pro vytváření, tj. oboje data musí být taková, aby ve spojení zajišťovala požadované funkce. Data pro ověřování elektronického podpisu se při použití technologie digitálního podpisu nazývají „veřejný klíč“ a data pro vytváření elektronického podpisu „soukromý klíč“. Tato data si každý zájemce generuje prostřednictvím aplikace pro generování klíčů. Data pro vytváření podpisu musí podepisující osoba uchovat v tajnosti, data pro ověřování podpisu jsou naopak určena ke zveřejnění. Data pro ověřování podpisu je nutné bezpečně předávat mezi podepisující osobou a osobou, která se na podpis spoléhá - zpravidla příjemce elektronicky podepsané zprávy. K tomuto bezpečnému předání může sloužit certifikát (viz příslušné heslo), což je datová zpráva, která spojuje data pro ověřování podpisu s osobou, které byl vydán (tj. s podepisující osobou) a umožňuje ověřit její totožnost.

Poskytovatelé nabízejí možnost vygenerovat data ve spolupráci s nimi, resp. umožňují jejich vygenerování. To však zpravidla neznamená, že poskytovatel data sám vygeneruje. V takovém případě by hrozilo nebezpečí, že pokud bude poskytovatel nedůvěryhodný a bude znát data pro vytváření elektronického podpisu osoby, které vydává certifikát, může je zneužít jako kdokoliv jiný.

Někteří poskytovatelé, zejména v zahraničí, nabízejí službu generování dat pro vytváření elektronického podpisu. Pokud by tuto službu měl v úmyslu nabídnout poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty podle zákona o elektronickém podpisu, musí mít na zřeteli ustanovení § 6 odst. 3 zákona, podle kterého „nesmí uchovávat a kopírovat data pro vytváření zaručeného elektronického podpisu osob, kterým poskytuje své certifikační služby“.

Úmysl získat certifikát se vyjádří vyplněním žádosti o vystavení certifikátu a jejím odesláním (předáním) poskytovateli. Součástí procesu vyplňování žádosti je generování dvojice dat pro vytváření a ověřování elektronického podpisu (asymetrických šifrovacích klíčů) v prostředí počítače žadatele o certifikát. Data pro vytváření elektronického podpisu zůstávají uložena u žadatele, data pro ověřování elektronického podpisu se stávají součástí žádosti o vydání certifikátu.

Data pro vytváření elektronického podpisu mohou být uložena na pevném disku počítače, na disketě, na čipové kartě nebo v přenosném bezpečnostním modulu (souhrnně „tokeny“). Je vhodné, aby přístup k těmto datům byl chráněn přístupovým heslem, frází, PINem apod., které zná jen jejich vlastník. Volba nosiče by měla odpovídat účelu, pro který bude elektronický podpisu používán.

§ 2 písm. i) zákona: daty pro vytváření elektronických podpisů (se rozumí) jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu

§ 2 písm. j) zákona: daty pro ověřování elektronických podpisů (se rozumí) jedinečná data, která se používají pro ověření elektronického podpisu

Datová zpráva

S pojmem „datová zpráva“ se lze v souvislosti s elektronickým podpisem setkat především ve dvou významech – datovou zprávou je to, co je podepisováno, datovou zprávou je i certifikát (viz příslušné heslo).

Elektronicky je možné podepsat jakoukoliv datovou zprávu, tedy vše, co existuje v elektronické (binární) podobě. Může to být e-mailová zpráva, obrázek, program, databázový soubor, makro atd.

§ 2 písm. c) zákona: datovou zprávou (se rozumí) elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou

Digitální podpis

Viz též **Elektronický podpis, Zaručený elektronický podpis, Data pro vytváření a data pro ověřování elektronického podpisu**

Technologie digitálních podpisů umožňuje vytváření zaručených elektronických podpisů podle zákona o elektronickém podpisu. K objasnění pojmu digitální podpis je nutné vysvětlit několik matematických a kryptografických technik. Na straně podepisující osoby se

z napsané zprávy pomocí hashovací funkce vytvoří tzv. otisk zprávy (anglicky „message digest“) – označme jej HASH 1. Na vstupu hashovací funkce může být libovolná a libovolně dlouhá datová zpráva, na jejím výstupu je otisk, který má pevnou délku 128 nebo 160 bitů (první údaj platí pro hashovací funkci MD5, druhý pro SHA-1, předpokládá se, že v krátké budoucnosti se začnou používat i hashovací funkce s otiskem s vyšším počtem bitů). Pokud by následně bylo ve zprávě změněno jediné písmeno, mezera mezi slovy nebo čárka ve větě, získá se na výstupu zcela jiný otisk. Výpočetně je prakticky nemožné vytvořit ke zprávě jinou zprávu, která má stejný otisk. Vytvořený otisk napsané zprávy se šifruje za pomoci zvoleného asymetrického algoritmu a pomocí dat pro vytváření elektronického podpisu osoby, která se podepisuje. Získaný výsledek je digitálním podpisem, který je ke zprávě připojen.

Na straně příjemce zprávy se k otevřenému textu vypočte hash – tentokráte jej označme HASH 2. Z digitálního podpisu se pomocí dat pro ověřování elektronického podpisu osoby, která zprávu podepsala, získá hodnota, která by se měla rovnat hodnotě HASH 1. Pokud jsou hodnoty HASH 1 a HASH 2 shodné, má osoba, která se na podpis spoléhá, jistotu, že zpráva nebyla cestou změněna a že zprávu podepsala osoba, které přísluší data pro vytváření elektronického podpisu, neboť jen ta mohla z HASH 1 vytvořit digitální podpis.
Uvedené postupy ani podepisující osoba ani příjemce zprávy na svém monitoru nevidí. Proces podepsání je spuštěn zadáním pokynu „digitálně (elektronicky) podepsat nebo např. ověřit podpis“.

Za předpokladu použití bezpečného podpisového schématu nelze odvodit či vypočítat z elektronického podpisu nebo z dat pro ověřování elektronického podpisu data pro jeho vytváření.

Zákon o elektronickém podpisu neužívá pojem digitální podpis, nýbrž zaručený elektronický podpis (viz). Přebírá tak princip Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy, tj. stanoví pojmy bez ohledu na technologii, která je v současné době používána. Předpokládá se, že v budoucnu budou využity například biometrické metody.

Elektronická podatelna

Elektronická podatelna je definována v nařízení vlády č. 304/2001 Sb. jako pracoviště pro příjem a odesílání datových zpráv. Povinnost zřídit jedno či více takových pracovišť je uložena tímto nařízením orgánům veřejné moci, pokud pro ně ze zvláštních předpisů, které jsou v tomto nařízení citovány pod čarou, vyplývá povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo těchto orgánů činit úkony v elektronické podobě. Tato povinnost se vztahuje rovněž na územní samosprávné celky provádějících výkon státní správy v rámci přenesené působnosti.

Elektronické podatelny musí být vybaveny potřebnými zařízeními připojenými k veřejné datové síti, popřípadě jiným sítím. Tato zařízení musí splňovat požadavky na technické a programové vybavení podle standardů vydaných Úřadem pro veřejné informační systémy. Zařízení musí umožňovat používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Elektronický podpis

Viz též **Digitální podpis, Zaručený elektronický podpis**

Elektronický podpis je zpravidla chápán jako číslo, které vytváří podepisující osoba pomocí svých dat pro vytváření elektronického podpisu a pomocí zprávy, kterou podepisuje. Elektronický podpis je jiný pro dvě odlišné zprávy, závisí na podepisované zprávě, nelze jej

tedy koupit ani jinak obdobně získat. Přísně vzato by se pod pojem „elektronický podpis“ vešel i podpis, který je napsán z klávesnice PC. Takový podpis příliš velkou důvěru nevzbuzuje - je těžké identifikovat a prokázat, kdo jej skutečně napsal. Elektronickým podpisem je tedy v praxi zpravidla míněn zaručený elektronický podpis. Ten umožňuje vytvářet technologie digitálních podpisů.

V případě, že zpráva byla podepsána zaručeným elektronickým podpisem:
-fyzická osoba (podepisující osoba), která zprávu podepsala, nemůže popřít, že je původcem této zprávy (nepopiratelnost původu – anglicky „non-repudiation“),
-je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána (zachování integrity zprávy, tj. její celistvosti),
-je možné zjistit identitu podepsané osoby,
-je zajištěna právní akceptovatelnost podpisu.

Uvedených vlastností zaručeného elektronického podpisu nemusí využít pouze příjemce zprávy, ale obecně kdokoliv, kdo se na daný podpis spoléhá. Příjemcem zprávy může být například příslušný finanční úřad jako příjemce daňového přiznání. Dalším, kdo se na daný zaručený elektronický podpis spoléhá, může být příslušný správce daně.
Na rozdíl od vlastnoručního podpisu, který je, resp. ideálně by měl být pokaždé stejný, a to bez ohledu na to, co se podepisuje, je zaručený elektronický podpis pokaždé jiný. Závisí na textu, ke kterému je připojen, a na použitých datech pro vytváření elektronického podpisu. To je důvodem, proč není možné mít podpisové vzory zaručených elektronických podpisů. Stejně tak nelze elektronicky podepsat zprávu dříve, než byla napsána („in bianco“), tj. zaručený elektronický podpis nemůže existovat sám o osobě, bez zprávy, kterou má podepsat.

§ 2 písm. a) zákona: elektronickým podpisem (se rozumí) údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě

§ 2 písm. b) zákona: zaručeným elektronickým podpisem (se rozumí) elektronický podpis, který splňuje následující požadavky:

- *je jednoznačně spojen s podepisující osobou,*
- *umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,*
- *byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,*
- *je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat*

Kvalifikovaný certifikát

Viz též **Certifikát**

Kvalifikovaný certifikát je certifikát, jehož obsah je stanoven zákonem o elektronickém podpisu (viz dále).

§ 2 písm. h) zákona: kvalifikovaným certifikátem (se rozumí) certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty

§ 12 zákona:
(1) Kvalifikovaný certifikát musí obsahovat:
a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,
c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
h) počátek a konec platnosti kvalifikovaného certifikátu,
i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,
j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(1) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

Kvalifikovaný (elektronický) podpis

Pojem kvalifikovaný podpis, resp. kvalifikovaný elektronický podpis neobsahuje ani zákon o elektronickém podpisu ani Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy. Poprvé se objevil v dokumentech, které vznikají z iniciativy Evropské komise a na směrnici navazují. Kvalifikovaným podpisem je míněn zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí použití prostředku pro bezpečné vytváření elektronického podpisu (viz Prostředek pro vytváření elektronických podpisů a prostředek pro ověřování elektronických podpisů). Tento „opis“ kvalifikovaného podpisu obsahuje zákon o elektronickém podpisu:

§ 3 odst. 2 zákona: Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

Zákon ani vyhláška neupravují, v jakých případech má být kvalifikovaný podpis používán.

Nástroj elektronického podpisu

Pojem nástroj elektronického podpisu se poprvé objevil v zákoně o elektronickém podpisu a byl převzat ze směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy (angl. electronic-signature product). Z nástrojů elektronického podpisu, jak jsou definovány v zákoně o elektronickém podpisum (viz dále), jsou ve středu pozornosti nástroje používané poskytovatelem pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny. Tyto nástroje nesmí poskytovatel používat pro jiné účely, jakými mohou být podepisování vydávaných certifikátů, které nejsou kvalifikovanými certifikáty podle zákona o elektronickém podpisu, podepisování jiných datových zpráv apod. Nástroje musí odpovídat požadavkům stanoveným zákonem o elektronickém podpisu a upřesněným vyhláškou k tomuto zákonu. Nástroj, který poskytovatel

hodlá pro uvedené účely používat, musí projít hodnocením Úřadu (viz § 8 vyhlášky č.366/2001 Sb. a příslušný komentář). Pokud poskytovatel hodlá používat nástroj, u nějž Úřad již shodu dříve vyslovil, není nutné nástroj opětovně hodnotit. Seznam nástrojů, u nichž byla vyslovena shoda, je zveřejňován ve Věstníku Úřadu a na webových stránkách Úřadu. Předpokládá se, a dosavadní krátká praxe tomu nasvědčuje, že o vyslovení shody budou žádat především dovozci či prodejci nástrojů, nikoliv sami poskytovatelé.

§ 2 písm. o) zákona: nástrojem elektronického podpisu (se rozumí) technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů

Osoba spoléhající se na podpis

Osobou spoléhající se na podpis může být příjemce elektronicky podepsané zprávy i osoba, která není přímým příjemcem zprávy od podepisující osoby, ale s elektroniky podepsanou zprávou pracuje a potřebuje se na podpis spoléhat (např. správce daně, auditor, soud apod.).
Osoba spoléhající se na podpis může využít skutečnosti, že většina běžně užívaných aplikací zasílá certifikát zároveň s elektronicky podepsanou zprávou. Pokud tomu tak není, musí podepisující osoba oznámit, kde je její certifikát dostupný, nebo musí být z použitého systému (nebo protokolu) zřejmé, kde se úložiště takovéhoto certifikátu nachází. Zpravidla se jedná o server poskytovatele, který certifikát vydal, nebo webovou stránku podepisující osoby. Nelze počítat s tím, že z certifikátu je možné obecně získat příliš mnoho informací o osobě, které byl vydán, tj. o podepisující osobě. To ostatně není účelem certifikátu. Účelem je důvěryhodným způsobem předat data pro ověřování elektronického podpisu podepisující osoby.

Osoba spoléhající se na podpis spoléhá na to, že poskytovatel před vydáním certifikátu ověřil totožnost osoby, které certifikát vydává. Při vydávání certifikátů nižších úrovní se neověřuje totožnost, ale například platnost a existence e-mailové adresy. Tento postup však nelze uplatnit v případě, že je vydáván kvalifikovaný certifikát podle zákona o elektronickém podpisu, kdy se jednoznačně požaduje ověření totožnosti žadatele o vydání kvalifikovaného certifikátu a pořízení kopie jeho průkazů totožnosti.

Je třeba připomenout, že poskytovatel certifikačních služeb nemůže jiné osobě, tedy ani osobě spoléhající se na podpis, sdělit údaje, které osoba, která žádá o vystavení certifikátu, tomuto poskytovateli sdělila (například poštovní adresa, telefonní číslo) a které nejsou uvedeny v certifikátu. Výjimku představují situace, kdy dotčená osoba vysloví se sdělením těchto údajů souhlas nebo pokud tak stanoví zákon (například v případě soudního řízení apod.).

Zákon o elektronickém podpisu neobsahuje pojem „osoba spoléhající se na podpis“ ani jiný obdobný pojem. K jejímu jednání, případně povinnostem se vztahuje zejména následující ustanovení:

§ 5 odst. 2 zákona: Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Ověření platnosti certifikátu

Pro ověření platnosti certifikátu podepisující osoby je nutným předpokladem důvěra v poskytovatele, který jej vydal. Pokud osoba spoléhající se na podpis tuto důvěru má, nainstaluje do svého software certifikát poskytovatele (je nutné odlišit certifikát poskytovatele a certifikát podepisující osoby).

Pokud osoba spoléhající se na podpis obdrží elektronicky podepsanou zprávu a zároveň certifikát podepisující osoby (případně získá certifikát jiným způsobem), následně ověří, zda certifikát podepisující osoby vydal poskytovatel uvedený v certifikátu a zda tento certifikát nebyl od okamžiku jeho vydání změněn. Toto ověření zajistí sama aplikace, a to ověřením elektronického podpisu poskytovatele, který je na certifikátu podepisující osoby.
Následně se zjišťuje, zda byl certifikát podepisující osoby platný v době, kdy byla zpráva podepsána. Přímo v certifikátu je uveden počátek a konec doby platnosti certifikátu (platnost od – do). V průběhu této doby však mohla být ukončena platnost certifikátu. Zda se tak nestalo, je nutné ověřit u poskytovatele v seznamu certifikátů, které byly zneplatněny (zveřejňován obvykle pod zkratkou CRL – Certification Revocation List – viz příslušné heslo).

Vždy je nutné počítat s určitým prodlením, které nastane mezi dobou, kdy držitel certifikátu požádá o ukončení platnosti svého certifikátu, a dobou, kdy je informace o zneplatnění certifikátu zveřejněna v CRL, resp. je vydán nový, aktualizovaný seznam zneplatněných certifikátů. Z technického i organizačního hlediska je velmi obtížné, aby mezi těmito dvěma akcemi nebyla určitá časová prodleva. Jak dlouhá tato prodleva je, lze zjistit v certifikační politice příslušného poskytovatele. Podle obsahu elektronicky podepsané zprávy je nutné zvážit, zda akceptovat obsah zprávy až poté, kdy uplyne doba, kterou poskytovatel potřebuje ke zveřejnění nového seznamu certifikátů, které byly zneplatněny. Například pokud osoba spoléhající se na podpis obdrží zprávu se závažným obsahem (zavazuje se, že uhradí 10 milionů Kč) a ví, že poskytovatel vydává nový seznam certifikátů, které byly zneplatněny (CRL), každých 12 hodin, je vhodné, aby s platbou vyčkala, než si ověří v CRL které bylo vydáno 12 hodin po podepsání dokumentu (nebo pokud není schopna prokázat, kdy byl dokument podepsán, 12 hodin po přijetí dokumentu) , že certifikát je stále platný.

Je-li ověřována platnost kvalifikovaného certifikátu, je nutné pamatovat na následující ustanovení:
§ 5 odst. 2 zákona: Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Podepisující osoba

Podepisující osobou ve smyslu zákona č. 227/2000 Sb. může být pouze fyzická osoba. Stejně jako v případě vlastnoručního podpisu není přípustné, aby se elektronicky podepisovala právnická osoba, byť v případě elektronického podpisu by z technického hlediska teoreticky taková možnost byla. Stejně jako jsou v organizaci (firmě apod.) určeni pracovníci, kteří jsou oprávněni svým podpisem opatřovat listinné dokumenty a jednat tak jménem právnické osoby, je potřeba analogicky postupovat i při elektronickém podepisování. V certifikátu v položce „účel“ lze konstatovat oprávnění fyzické osoby k podepisování jménem osoby právnické. Fyzická osoba se tak může elektronicky podepisovat jménem právnické osoby a osoba spoléhající se na podpis v certifikátu „vidí“, že tato osoba je k tomu oprávněna.

Podepisující osoba musí mít prostředek pro vytváření elektronického podpisu (viz Prostředek pro vytváření a prostředek pro ověřování elektronických podpisů) a data pro vytváření elektronického podpisu (viz Data pro vytváření a data pro ověřování elektronického podpisu).

Bezpečnost elektronického podepisování je do značné míry závislá na chování podepisující osoby, zejména na její schopnosti uchovat v tajnosti svá data pro vytváření elektronického podpisu (soukromý klíč). Pokud hrozí nebezpečí zneužití jejích dat pro vytváření elektronického podpisu, je podepisující osoba o této skutečnosti povinna uvědomit poskytovatele, který jí kvalifikovaný certifikát vydal. Další povinností podepisující osoby je podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu. I když zákona stanoví uvedené povinnosti pouze v případě, že je vydán certifikát s označením „kvalifikovaný" a jedná se o kvalifikovaný certifikát podle zákona, je žádoucí, aby se takto podepisující osoba chovala i v případě, že jí byl vydán jakýkoliv certifikát.

Fyzická osoba může mít libovolný počet certifikátů. Jiné certifikáty může akceptovat banka, jiné úřad. S „univerzálními" certifikáty, které by akceptovali všichni potenciální příjemci elektronicky podepsaných zpráv (všechny osoby spoléhající se na podpis), se v současné době ani v ČR ani zahraničí nepočítá. Je to obdobná situace, jako když osoba využívá služeb více bank a od každé má jednu platební kartu.

§ 2 písm. d) zákona: podepisující osobou (se rozumí) fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby

§ 5 odst. 1 zákona: Podepisující osoba je povinna
-zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
-uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,
-podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

Poskytovatel certifikačních služeb

Viz též **Certifikační autorita**

Poskytovatel certifikačních služeb je subjekt, který vydává certifikáty a vede jejich správu. Zejména zveřejňuje seznamy vydaných certifikátů a seznamy certifikátů, které byly zneplatněny (CRL viz Certificate Revocation List). Přijímá a realizuje žádosti o ukončení platnosti certifikátů.

V České republice působí těchto poskytovatelů několik a s nabídkou jejich služeb a s praktickými návody jejich využití je možné se seznámit na jejich webových stránkách. Někteří z těchto poskytovatelů vydávají certifikáty již několik let. Předmětem jejich služeb není poskytování elektronických podpisů, jak se někdy mylně uvádí, ale vydávání certifikátů a další výše uvedené činnosti. Certifikáty jsou vydávány zpravidla na dobu šesti měsíců a za cenu několika stokorun.

Ti poskytovatelé certifikačních služeb, kteří se rozhodnou, že budou vydávat kvalifikované certifikáty podle zákona o elektronickém podpisu (viz Kvalifikovaný certifikát), se musí řídit příslušnými ustanoveními tohoto zákona.
Poskytovatelé se mohou rozhodnout, že požádají Úřad (viz Úřad pro ochranu osobních údajů) o udělení akreditace (viz Akreditace). Činnost akreditovaných poskytovatelů je podle příslušného ustanovení zákona o elektronickém podpis nezbytná v „oblasti orgánů veřejné moci", kde „je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb".

Nad činností akreditovaných poskytovatelů a poskytovatelů vydávajících kvalifikované certifikáty vykonává Úřad dozor.

To neznamená, že všichni poskytovatelé musí vydávat kvalifikované certifikáty, případně žádat o akreditaci, a všichni občané, kteří se chtějí elektronicky podepisovat, musí mít kvalifikované certifikáty. V soukromoprávní oblasti, například při komunikaci dvou firem, komerčních bank s jejich klienty apod. je na komunikujících subjektech, zda budou vyžadovat používání kvalifikovaných certifikátů ve smyslu zákona o elektronickém podpisu.
Při výběru poskytovatele jsou základními hledisky zpravidla:
jeho důvěryhodnost,
účel, pro který bude elektronický podpis používán,
služby, které poskytovatel nabízí,
kompatibilita s aplikacemi, které žadatel o certifikát používá,
cena poskytovaných služeb.

Pro některé účely může plně postačit certifikát, při jehož vydání žadatel komunikuje s poskytovatelem pouze e-mailem. Vydání takového certifikátu nabízejí jak zahraniční tak tuzemští poskytovatelé na svých webových stránkách. Vydávání těchto certifikátů je zpravidla zdarma.

Pro jiné účely, např. pro styk s bankou nebo úřadem, bývá vymezen okruh poskytovatelů, jejichž certifikáty daný subjekt (banka, úřad) uznává. Například banky uznávají většinou pouze ty certifikáty, které samy vydaly. Získání certifikátu, který má poskytnout vyšší míru záruky a který je určen pro komunikaci v závažných věcech (finanční operace, podání, smluvní závazky apod.), a to včetně kvalifikovaného certifikátu podle zákona, je spojeno s ověřováním totožnosti osoby, které má být certifikát vydán. Je tedy nezbytné poskytovatele s příslušnými osobními doklady osobně navštívit. V případě vydání kvalifikovaného certifikátu je poskytovatel navíc povinen pořídit a uchovat kopie dokladů, kterými se totožnost prokazuje.

Poskytovatelé velmi často nabízejí zdarma vydávání testovacích certifikátů. K jejich vydání není nutná osobní návštěva poskytovatele.

Zákon o elektronickém podpisu podrobně a v mnoha ustaveních upravuje povinnosti poskytovatelů, kteří vydávají kvalifikované certifikáty, resp. akreditovaných poskytovatelů. Připomeňme alespoň příslušné definice:
§ 2 písm e) zákona: poskytovatelem certifikačních služeb (se rozumí) subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy

§ 2 písm. f) zákona: akreditovaným poskytovatelem certifikačních služeb (se rozumí) poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona

Prostředek pro vytváření elektronických podpisů a prostředek pro ověřování elektronických podpisů

Uvedené pojmy se poprvé objevily v zákoně o elektronickém podpisu a byly převzaty ze směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy (angl. signature-creation device, signature-verification device). Souhrnně se jedná o hardware a software, které jsou užívané pro vytváření, resp. ověřování elektronických podpisů. Náležitosti a způsob používání těchto prostředků zákon o elektronickém podpisu neupravuje.

Z hlediska bezpečnosti lze za prostředky vyšší kategorie označit prostředky pro bezpečné vytváření elektronických podpisů a prostředky pro bezpečné ověřování elektronických podpisů (oproti výše uvedeným pojmům je vloženo slovo „bezpečné“, angl. secure-signature-creation device, pro prostředek pro bezpečné ověřování směrnice odpovídající pojem neobsahuje, pouze v příloze IV uvádí doporučení pro bezpečné ověření

podpisu). Požadavky na tyto prostředky jsou stanoveny v § 17 zákona a upřesněny v § 7 vyhlášky. Povinnost používat tyto prostředky zákon ani vyhláška nestanoví. Více k tomuto tématu viz komentář k § 7 vyhlášky.

§ 2 písm k) zákona: prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů

§ 2 písm. l) zákona: prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů

§ 2 písm. m) zákona: prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem

§ 2 písm. n) zákona: prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem

Příjemce datové zprávy – viz **Osoba spoléhající se na podpis**

Registrační autorita

Vykonává regitrační služby, tj. zejména ověřuje totožnost osob, které žádají o vydání certifikátu, případně zjišťuje specifické znaky těchto osob. Tato služba předchází vydání certifikátu. Může zahrnovat rovněž ověření, zda žadatel o vydání certifikátu má data pro vytváření podpisu. Registrační autorita je místem, kde se uzavírá s žadateli smlouva o vydání certifikátu a kde je dostupná certifikační politika (viz Certifikační politika) a certifikát poskytovatele Pro zajišťování činnosti registračních autorit certifikační autority často využívají služeb jiných subjektů, tj. děje se tak na základě smluvních vztahů mezi certifikační autoritou a registrační autoritou. Viz též Certifikační autorita.

Zákon o elektronickém podpisu neupravuje výslovně činnost registračních autorit, ale povinnosti, které se na činnosti, které zpravidla zajišťují, vztahují, jsou obsaženy v povinnostech poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty (zejména § 6 zákona).

Seznam certifikátů, které byly zneplatněny – viz **Certification revocation list (CRL)**

Šifrování

Šifrování datové zprávy je samostatný úkon, který nevyplývá z funkce elektronického podpisu. Elektronicky podepsaná zpráva může být šifrována, ale toto šifrování nezajišťuje elektronický podpis. Pokud tedy elektronicky podepsaná datová zpráva není šifrována, je předávána v otevřené podobě a osoba, která ji získá, se může seznámit s jejím obsahem.
Zákon o elektronickém podpisu šifrování elektronicky podepsaných datových zpráv neupravuje.

Time stamping – viz **Časové razítko**

Úřad pro ochranu osobních údajů (ÚOOÚ)

Informace o Úřadu pro ochranu osobních údajů lze získat na Internetové adrese http://www.uoou.cz .

Povinnosti, příp. kompetence Úřadu v oblasti elektronického podpisu stanoví celkem tři právní předpisy: zákon o ochraně osobních údajů, zákon o elektronickém podpisu a vyhláška k tomuto zákonu. Základními povinnostmi Úřadu jsou udělování (a případné odnímání) akreditací, dozor nad činností akreditovaných poskytovatelů a poskytovatelů vydávajících kvalifikované certifikáty, vyhodnocování shody nástrojů elektronického podpisu a vydávání vyhlášek podle § 20 zákona o elektronickém podpisu. Úřad naopak nekoordinuje používání elektronického podpisu v ČR, a to ani v případě elektronické komunikaci mezi občanem a státem.

§ 2 odst. 2 zákona č. 101/2000 Sb. o ochraně osobních údajů: Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a pro oblast elektronického podpisu v rozsahu stanoveném zvláštním právním předpisem (pozn. tj. zákonem o elektronickém podpisu)

§ 9 odst. 1 zákona: Udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb, jakož i dozor nad dodržováním tohoto zákona náleží Úřadu.

§ 9 odst. 2 zákona: (Úřad)
písm. a): uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky,
písm. b): vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona (atd.)
písm. e): vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou (atd.)

Zaručený elektronický podpis
Více viz **Elektronický podpis**

Vytváření zaručených elektronických podpisů umožňuje technologie digitálních podpisů (viz Digitální podpis).
Zaručený elektronický podpis, pro který se v praxi ne zcela přesně často používá zkrácený název elektronický podpis, definuje zákon o elektronickém podpisu následovně:
§ 2 písm. b) zaručeným elektronickým podpisem (se rozumí) elektronický podpis, který splňuje následující požadavky:
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX část 1.

Jaroslav Pinkava, AEC spol. s r.o.

1. Úvod

Předchozí části seriálu Kryptografie a normy byly věnovány problematice digitálních certifikátů. Stručný úvod do problematiky (Crypto-World 9/2002) byl následován popisem normy X.509 (verze 3 – Crypto-World 10/2002 resp. novější verze 4 – Crypto-World 11/2002). Pro práci s digitálními certifikáty je v praxi vytvářen bohatý software, který je dle konkrétních zámyslů vývojářů a potřeb uživatelů implementací celé řady algoritmů, protokolů, postupů atd. K tomu, aby tyto postupy mohly být ujednoceny (a tím například zajištěna kompatibilita softwaru různých vývojářů) jsou zpracovávány různorodé normativní dokumenty. Velice užitečnou práci v tomto směru odvádí pracovní skupina IETX – PKIX.

Tato skupina byla ustavena již v roce 1995. První prací bylo zpracování profilu certifikátu veřejného klíče dle normy X.509 (existovalo postupně jedenáct draftů, pak vzniklo RFC 2459; i toto RFC je ale předmětem obdobně dlouhé řady dalších úprav) . Řada dokumentů zpracovaných skupinou byla schválena IESG (The Internet Engineering Steering Group) a existuje jako RFC. Základním z těchto dokumentů je RFC 2459 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), který, jak již název napovídá, definuje profily certifikátů a CRL. Zpracovány jsou dokumenty k dvěma typům řídících protokolů (CMP a CMC), OCSP protokol a další – budou popsány níže. V současné době jsou připravovány dokumenty orientované na spolupráci s PKI, využití PKI apod. Jsou připravovány alternativní cesty k odvolávání certifikátů, postupy pro využití tzv. kvalifikovaných certifikátů (rozšíření těchto certifikátů), využití časových značek, podpora nepopiratelnosti. Zpracovávány jsou postupy pro práci s atributovými certifikáty.

Celkový přehled o dokumentech skupiny poskytuje materiál draft-ietf-pkix-roadmap-07.txt (Internet X.509 Public Key Infrastructure:Roadmap). V tomto úvodním dílu (z hlediska IETF-PKIX) bude proto použit pro vstupní informaci. Veškeré dokumenty skupiny lze nalézt na adrese: http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

2. K základnímu členění dokumentů IETF-PKIX

V příloze článku je uveden seznam dokumentů skupiny, tak jak existoval na počátku března 2002. Již z počtu a ze samotných názvů dokumentu je vidět široký záběr pracovních témat a variabilita jejich zaměření. Vše je však orientováno na podporu PKI a PMI s využitím normy X.509.

Prvotní úsilí skupiny zaměřené na vytvoření obecně přijímaného profilu certifikátu (veřejného klíče) bylo následováno vývojem protokolů nezbytných pro řízení informací, které se vztahují k PKI. Prvním z těchto protokolů Byl protokol CMP (Certificate Management Protocol). Tento definoval zprávy vztažené k inicializaci, certifikaci, obnově a odvolávání entit PKI. Dvě pracovní skupiny (IETF-S/MIME a IETF-PKIX) vyvinuly dva různé dokumenty vztahující se k žádostem o certifikát. CRS (Certificate Request Syntax) vyvinula skupina S/MIME, která přitom použila formát dle PKCS-10 (viz dřívější části seriálu Kryptografické normy v Crypto-Worldu). Jiný typ formátu CRMF (Certificate Request Message Format) vyvinula skupina PKIX. Tento se opírá jak o CMP tak i o přihlášení dle CRS, ale nepoužívá formát žádosti dle PKCS-10.

Protokol CMC pak napomáhá využívání protokolu pracovní skupiny S/MIME pro řízení PKI bez nutnosti využití CMP (používá PKCS-10). Souvisí pak s tím i zpracování

transportního protokolu TCMP (Transport Protocols for CMP), kde je popsáno jak využití http, tak i TCP (Trannsmission Control Protocol).

Problematikou odvolávání (revokace) certifikátů se zabývá OCSP (Online Certificate Status Protocol). Tento protokol definuje online mechanismus pro zjištění statutu certifikátu veřejného klíče (což může být aktuálnější informací než je informace obsažená v CRL). Protokol SCVP (Simple Certification Verification Protocol) umožňuje spoléhajícím se stranám přesunout veškerou nezbytnou verifikaci certifikační cesty na jinou entitu. Na oba dokumenty navázaly další drafty. Byla definována (ve vztahu k SCPV) nová rozšíření pro OCSP (OCSPv2) a problematikou se zabývali i drafty DPV (Delegeted Path Validation) a DPD (Delegated Path Discovery).

Jiným dokumentem vztahujícím se k statutu certifikátu je OCDP (Open CRL Distribution Point). Pro využití LDAP (Light Weight Directory Access Protocol) vznikly postupně čtyři různé dokumenty; jeden pro definování LDAPv2 jako přístupového protokolu do repozitářů; dva pro ukládání PKI informace v adresářích a jeden pro požadavky LDAPv3.

Následovala řada dokumentů, která se týká protokolů vztahujících se k využívání časových značek – interakce s časovou autoritou.

Nově se (v návaznosti i na čtvrtou verzi X.509) se objevily drafty zabývající se problematikou atributových certifikátů (profil certifikátu a související protokol pro přístup do repozitáře).

Speciální problematikou se zabývá draft definující dva mechanizmy pro vytváření podpisu z dvojice klíčů DH (Diffie-Hellman). Další speciální dokumenty se zabývají kvalifikovanými certifikáty a tzv. stálým identifikátorem (Permanent Identifier).

Jednotlivými okruhy dokumentů se budeme zabývat v návazných článcích.

3. Terminologie použitá v dokumentech IETF-PKIX

Atributová autorita (AA) – autorita, důvěryhodná instituce, vytvářející a podepisující atributové certifikáty. Atributová autorita zodpovídá za atributové certifikáty během jejich celého životního cyklu, nejen za jejich vydávání.

Atributový certifikát (AC) – struktura dat obsahující množinu atributů a další informace. Tato struktura je podepsána soukromým klíčem AA, která certifikát vydala.

Certifikát – zde buď atributový certifikát nebo certifikát veřejného klíče.

Certifikační autorita (CA) - autorita, důvěryhodná instituce, vytvářející a podepisující certifikáty veřejných klíčů. Certifikační autorita zodpovídá za atributové certifikáty během jejich celého životního cyklu, nejen za jejich vydávání. Někdy může i vytvářet klíče uživatelů.

Certifikační politika (CP) – množina pravidel, která indikuje využitelnost certifikátu veřejného klíče pro určitý okruh aplikací se společnými bezpečnostními požadavky (např. v rámci elektronického obchodu pro autentizaci určitého typu transakcí).

Certifikační prováděcí směrnice (CPS) – Směrnice obsahující postupy, kterými se řídí Ca vydávající certifikáty veřejných klíčů.

Konečná entita (end-entity - EE) – subjekt certifikátu, který není ani AA v PMI ani CA v PKIC. Poznámka: EE z PKI může být AA v PMI.

Certifikát veřejného klíče (PKC) – datová struktura obsahující veřejný klíč konečné entity a další informace. Tato struktura je podepsána soukromým klíčem CA, která certifikát vydala.

Infrastruktura veřejného klíče (PKI) – množina obsahující hardware, software, lidi, politiky a postupy, které jsou nezbytné k vytváření, řízení, ukládání, distribuování a odvolávání PKC založená na kryptografii veřejného klíče.

Infrastruktura řízení privilegií (PMI) – Soubor atributových certifikátů spolu s AA, které je vydávají, subjekty, spoléhající se strany a repozitáře.

Registrační autorita (RA) – Nepovinná entita, které byla udělena odpovědnost za provádění administrativních činností při registraci subjektů: ověřování totožnosti subjektu, vyhodnocení zda subjekt je oprávněn mít přiřazeny hodnoty uvedené v PKC a ověření, že subjekt vlastní soukromý klíč asociovaný s veřejným klíčem uvedeným v žádosti o PKC.
Spoléhající se strana – uživatel či agent (např. klient či server), který se spoléhá při provádění rozhodnutí na data v certifikátu.
Kořenová certifikační autorita - certifikační autorita, které EE přímo důvěřuje, tj. je zde nezbytný určitý krok navíc (bezpečné získání hodnoty veřejného klíče kořenové certifikační autority). Tj. kořenová autorita nemusí být autoritou, která je na vrcholu hierarchie, ale je tou autoritou, které je bezprostředně důvěřováno.
Podřízená certifikační autorita – taková autorita, která pro EE není kořenovou autoritou.
Subjekt - entita (AA, CA či EE) pojmenovaná v certifikátu (ať již PKC či AC). Subjektem může být člověk, počítač (reprezentovaný jmény dle DNS či IP adresou) nebo také softwarový agent.
Autorita časových značek (TSA) – důvěryhodná třetí strana, která dává důkaz existence v určitém časovém momentu.
Vrcholová certifikační autorita - certifikační autorita na vrcholu hierarchie PKI.

Příloha. Přehled existujících dokumentů (březen 2002)

Internet X.509 Public Key Infrastructure:Roadmap (146835 bytes)
An Internet Attribute Certificate Profile for Authorization (92528 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3 (16654 bytes)
Simple Certificate Validation Protocol (SCVP) (45297 bytes)
Internet X.509 Public Key Infrastructure Certificate and CRL Profile (294883 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (202678 bytes)
Internet X.509 Public Key Infrastructure Permanent Identifier (19078 bytes)
Transport Protocols for CMP (22793 bytes)
Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs (71516 bytes)
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile (53020 bytes)
Online Certificate Status Protocol, version 2 (54103 bytes)
PostScript version [159488 bytes].
Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) (49976 bytes)
Certificate Management Messages over CMS (57183 bytes)
Certificate Management Messages over CMS (95994 bytes)
Internet X.509 Public Key Infrastructure Proxy Certificate Profile (100318 bytes)
Delegated Path Validation and Delegated Path Discovery Protocols (47311 bytes)
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (138444 bytes)
CMC Transport (11041 bytes)
CMC Extensions: Server Side Key Generation and Key Archival (39886 bytes)
CMC Compliance Document (10457 bytes)
Internet X.509 Public Key Infrastructure Logotypes in X.509 certificates (26551 bytes)
Supplemental Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile (51737 bytes)
Delegated Signature Validation Delegated Path Validation and Delegated Path Discovery Protocol Requirements (39245 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP (25585 bytes)
Delegated Signature Validation Protocol Requirements (DSV-REQ) (27337 bytes)
Delegated Path Validation and Delegated Path Discovery Protocol Requirements (DPV&DPD-REQ) (34152 bytes)
Out-of-Band Certificate and Key Identifier Protocol (OCKID) (16529 bytes)
Attribute Certificate Request Message Format (16069 bytes)
Attribute Certificate Management Messages over CMS (20232 bytes)

X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (45537 bytes)
X.509 Extensions for IP Addresses and AS Identifiers (44450 bytes)

Request For Comments

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459) (278438 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510) (158178 bytes)
Internet X.509 Certificate Request Message Format (RFC 2511) (48278 bytes)
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527) (91860 bytes)
Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528) (18273 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559) (22894 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585) (14813 bytes)
Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587) (15102 bytes)
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) (43243 bytes)
Certificate Management Messages over CMS (RFC 2797) (103357 bytes)
Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875) (45231 bytes)
Internet X.509 Public Key Infrastructure Qualified Certificates Profile (RFC 3039) (67619 bytes)
Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (RFC 3029) (107347 bytes)
Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP) (RFC 3161) (54585 bytes)

C. Bezpečnost RSA – význačný posun?

Jaroslav.Pinkava, AEC spol. s r.o.

Známý americký kryptolog Daniel J. Bernstein již loni v srpnu na konferenci Crypto 2001 oznámil nový design pro počítač realizující metodu NFS (Number Field Sieve). Toto je v současné době nejefektivnější algoritmus pro faktorizaci velkých čísel (byl například úspěšně použit pro faktorizaci čísla v délce 512 bitů – viz starší čísla Crypto-Worldu; současný rekord je 524 bitů).

Z adresy http://cr.yp.to/papers/nfscircuit.ps lze získat jeho poslední článek na toto téma:
Circuits for integer factorization: A proposal. Při seznámení se s obsahem článku lze zjistit, že se nejedná o nový a zásadní objev, ale o optimalizaci známých technik používaných při metodě síta číselného tělesa. Je přitom nezbytné využití přídavného hardwaru pro zefektivnění různých implementačních neoptimalizovaných technik. Dle některých komentátorů kolují např. pověsti, že „třípísmenková agentura“ již obdobný přístroj vlastní. Článek Bernsteina je pak potvrzením možnosti existence takovéhoto specializovaného zařízení.

Pro přiblížení – při délce modulu ***n*** 1024 bitů vyžaduje klasické NFS čas 2^86 a paměť 2^43. Bernsteinovo NFS vyžaduje čas v řádu 2^53 při nárocích na paměť o velikosti 2^36. Podstatou Bernsteinových „vylepšení“ je využití paralelních výpočtů.

Bernstein sám zatím jím popisovanou technologii sám nerealizoval, ale dle dostupných informací jedná např. s organizátory známé každoroční konference Financial Cryptography (v letošním roce se koná v březnu na Bermudách) o poskytnutí potřebných finančních subvencí.

Podle předběžných odhadů se takto posun bezpečné délky parametrů RSA (délky ***n*** – součinu dvou prvočísel) dostává nad hranici 2000. Tj. doporučení zde vyplývající (dle komentátorů) – nepoužívat již dnes RSA z délkou ***n*** kratší než 2048 bitů a doporučuje se pro dlouhodobou bezpečnost připravovat implementace umožňující používat ***n*** alespoň v délce 8192 bitů.

Samozřejmě je nutné vyčkat s objektivním hodnocením až na výsledky příslušných experimentů. Avšak již dnes se objevují různé spekulace co s RSA a vůbec s asymetrickou kryptografii v budoucnu. Jedni doporučují přejít v co nejkratší době na kryptografii na bázi eliptických křivek. Jiní (možná příliš vystrašení tímto výsledkem, který může mít dopad na obrovskou řadu praktických aplikací) doporučují využívat pro asymetrickou kryptografii kombinované systémy. Tj. např. každý by měl nezávislé dvojice klíčů pro dva až tři asymetrické kryptosystémy (RSA a EC resp. další kryptosystém) a šifrování (dešifrování) by použilo postupně každý s těchto systémů.

Poznámka: Na konferenci ve Waterloo (říjen 2001) zástupce NSA hovořil o tom, že agentura převádí citlivá data na ECC (Elliptic Curve Cryptography).

D. TERMINOLOGIE II.

Vlastimil Klíma, ICZ a.s., (vlastimil.klima@i.cz)
archiv článků o bezpečnosti a šifrování:
http://www.decros.cz/bezpecnost/_kryptografie.html

(Se svolením Dr. Klímy uvádíme jeho odpovědi z diskuse v konferenci security@underground.cz . První část, na níž toto pokračování navazuje, byla uveřejněna v předchozím čísle.)

Dotaz : Který výraz používat pro "hash fuction"?
? haš, hash, hashovací funkce, hašovací funkce, otisk, fingerprint, miniatura (termín použitý v produktech Microsoftu) ?
Odpověď :
Já osobně bych souhlasil s haš, hash, hashovací funkce, hašovací funkce, otisk, hašovací kód, ostatní dva (fingerprint a miniatura) bych nebral.

Dotaz:
Encryption = šifrování, budiž bez námitek. Věda, která se tímto výzkumem zabývá ale není šifrologie či podobně, ale kryptologie (proč najednou opět kryptujeme?)? Nebo je kryptologie vědou, která to vše zastřešuje (což si myslím je spíše matematická algebra) a vše ostatní (včetně šifrování) jsou její 'podobory'?
Odpověď :
Moc zajímavé otázky. Opět jsem se obrátil na Ústav pro jazyk český. Takže: To, že se nepoužívá šifrologie namísto kryptologie, cituji "nemá žádný logický důvod, je to jen otázka konvence" a "šifrologie je nespisovné, spisovné je kryptologie". I když se Ústav, jak jsem již dříve psal, brání vyjádřením spisovné/nespisovné, v tomto případě jasně označil šifrologii za nespisovný výraz. Nehledejte tedy v tom logiku, ale vývoj jazyka. Jak jsem byl poučen, sloveso (šifrovat), vyjadřující činnost (šifrování) se nemusí nutně promítat do názvu vědy, která tuto činnost zahrnuje (kryptologie). Určitě najdete i další příklady v češtině. K další

podotázce: kryptologie pochází z řeckého slova kryptos (což znamená skrytý). V současné době se ustálilo, že kryptologie se skládá z kryptoanalýzy a kryptografie. Kryptografie zahrnuje nejen tvorbu šifer, ale i hašovacích funkcí, autentizačních a identifikačních schémat, kryptografických protokolů a spousty dalších kryptografických technik. Kryptoanalýza dnes neznamená jen přímé luštění šifer, ale hledání jejich slabostí nebo nevhodných vlastností, slabin protokolů, modů činnosti šifer a mnoha dalších kryptoanalytických technik. Kryptologie je tedy opravdu dnes chápána jako věda, která to vše zastřešuje.

Pro zájemce o jazykové oříšky: jazyková poradna, telefon 02/57531793 od 10 do 12 hod. nebo poradna@ujc.cas.cz .

Snad jedna příhoda navíc neuškodí:
Když mi jednou někdo přinesl v nějakém reklamním materiálu překlad slova šifrovat jako cypher, řekl jsem mu, že je to blbost. Pak mi ale přinesl slovník, a bylo to tam černé na bílém - cipher a cypher jsou synonyma ! (i když se cypher a z něho odvozená slova používají zřídka). Takže o překvapení není nouze. K historii slov cipher/crypt/apod. více možná na www.google.com , který vás zavede například na
http://www.angelfire.com/la/paw/cipher.html
http://www.hyperdictionary.com/dictionary/cypher
http://www.its.bldrdoc.gov/projects/t1glossary2000/_encrypt.html

E. Letem šifrovým světem

1. O čem jsme psali v březnu roku 2000 a 2001

Crypto-World 3/2000

Crypto-World 3/2001

2. Encryption in corporate networks can be 'pried open'

Václav Vopravil (Vaclav.Vopravil@siemens.com)

Při používání šifrovacích Pluginů (všechny verze, včetně PGP) do MS Outlooku (všechny verze), při standardní instalaci s MS Exchange serverem, může v lokální síti

docházet k nezabezpečené komunikaci. Je to způsobeno komunikací klientské části a serverové prostřednictvím protokolu RPC.

Týká se to třeba přípravy e-mailu, kdy tento návrh datové zprávy je kódován RPC, ale není zašifrován Pluginem při přenosu na MS Exchange server, kde je standardně uložena složka pošty k odeslání. MS Outlook ukládá zprávu na pozadí (Background Save), při odesíláni zprávy Plugin obdrží od MS Outlooku Event "OnWriteComplete", načež zprávu šifruje a potom šifrovanou odešle. To se samozřejmě týká i dopisu s přílohami, ale týká se to také příjemce pošty.

Možná řešení:

1. V registrech nastavit hodnotu DisableBGSave
2. šifrovani RPC nebo IPSec
3. používat IMAP/POP3/SMTP (ne MAPI)
4. používat MS Outlook v offline modu

a asi vás napadnou i další řešení...

Podle posledních zpráv Microsoft neplánuje hotfix, ale pravděpodobně k tomu bude donucen, platí totiž v několika zemích již zákony o elektronických podpisech.

Vyjádření MS lze nalézt zde:
http://www.microsoft.com/germany/ms/net-server/exchange/2000/crypto.htm
Poslední zpráva je zde http://www.heise.de/newsticker/data/pab-06.03.02-001/

3. ISO-registr kryptografických algoritmů byl zpřístupněn On-Line!

Tento registr slouží pro účely - JTC 1, ISO a IEC. Zpřístupněn byl na adrese http://www.iso-register.com/ . Registr spravuje professor Chris Mitchell (Royal Holloway, University of London, United Kingdom)

Registr je též dostupný z veřejné stránky SC-27 (http://www.din.de/ni/sc27). Tuto stránku spravuje Krystyna Passia (Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung e.V., Berlin , Germany).

4 . Velikonoční kryptobesídka

Vážené kryptoložky a vážení kryptologové,

rádi bychom Vás pozvali na workshop **Velikonoční kryptobesídka**, který se koná 3. - 4. dubna 2002 v Brně v nové budově Moravské zemské knihovny, Kounicova 65.

Můžete se zaregistrovat pomoci on-line formuláře, e-mailem nebo klasickým papírovým formulářem.

Program workshopu je uveden na webové http://www.ecom-monitor.cz/velikonoce
Za programový a organizační výbor

Pavel Vondruška, Vašek Matyáš a Zdeněk Říha

5. Uľahčí elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti, Jaroslav.Pinkava, AEC spol. s r.o.

Dne 20.2.2002 se v bratislavském hotelu Děvín konala konference zaměřená na využití elektronického podpisu. Organizátorem konference byl New Management Conferences - NMC s.r.o. (paní Gabriela Stuchlá - http://www.nmc.sk/). Konference se zúčastnila řada slovenských i českých odborníků pro tuto problematiku.

(na snímku zleva doprava: J. Pinkava, V. Smejkal, R. Rexa)

V příspěvcích se odrazily aktuální otázky související s přípravou slovenského zákona o elektronickém podpisu včetně vystoupení zástupců obou existujících názorových skupin. Zástupce EU pan Petersen vystoupil s povšechným příspěvkem, práce na problematice elektronického podpisu v SR i v ČR jsou již poněkud dále. Organizátoři konference pozvali celou řadu českých odborníků – proto zde zazněla i celá řada příspěvků, které se dotknuly aktuálních otázek problematiky el. podpisu v ČR. Podnětná byla vystoupeni P. Staši (elektronické podatelny), I. Svobody (čipové karty), L. Capouškové (k I.CA). Docent V. Smejkal obhajoval jím zvolený přístup při přípravě českého zákona o EP (Uncitral atd.). J. Pinkava (autor tohoto příspěvku) se zabýval některými problémy při zavádění zákona o EP do praxe. Mimo jiné upozornil na neexistenci české legislativy pro oblast kryptografie řešící ochranu neutajovaných dat (kryptografickou ochranu utajovaných dat pokrývá zákon 148/1998 Sb.).

Na závěr konference se konala panelová diskuse. Dotkla se celého širokého spektra elektronického podpisu, vystupující odpovídali na otázky jak teoretického tak i aplikačního charakteru.

6. Seminář GnuPG, 5. 4. 2002 v Praze

Roman Pavlík, (rp@tns.cz)

Vážení uživatelé PGP,

s potěšením Vám mohu oznámit, že pan Werner Koch, autor GnuPG (freewarové implementace OpenPGP) přijal naše pozvání a začátkem dubna navštíví vůbec poprvé Českou republiku.

Díky pochopení České společnosti uživatelů otevřených systémů - EurOpen.CZ se dne 5. 4. 2002 uskuteční v Praze celodenní seminář na téma GNU Privacy Guard.

Hlavní příspěvek přednese pan Koch. Součástí příspěvku bude mimo jiné rozbor kompatibility GnuPG/PGP, což je téma častých dotazů nejen této konference. Hlavní pozornost bude věnována architektuře GnuPG (bude popsána modularita GnuPG a způsob jak lze snadno GnuPG doplnit o další algoritmy pro šifrování/hashování).

Pozornost bude věnována i frontendům pro GnuPG. Pan Koch přislíbil také poodhalit něco z plánovaných změn pro GnuPG, hovořit bude i o projektech, které na GnuPG navazují.

V závěru odpolední části je připravena panelová diskuze. Pozvání přijal i pan Tomáš Rosa z ICZ a je tedy zřejmé, že hlavním tématem bude chyba formátu OpenPGP. Účastníci semináře tak budou mít jedinečnou možnost zúčastnit se odborné diskuze na toto téma a s odstupem času najít kvalifikovaný popis celého problému.

Příspěvek pana Kocha bude přednesen v angličtině. Můj úvodní příspěvek bude samozřejmě v češtině, při panelové diskuzi bude zajištěn tlumočník, který bude překládat dotazy publika z češtiny do angličtiny.

Pokud se na seminář přihlásíte a platbu provedete do 29. 3. 2002, je výše vložného 490,- Kč, pro studenty s platným indexem pak 190,- Kč. Po tomto termínu je vložné o 100,- Kč vyšší.

Každý účastník semináře obdrží tištěnou verzi manuálu Gnu Privacy Guard v angličtině. V ceně semináře je zahrnut i oběd (bez nápojů).

Bližší informace a přihlášku s postupem registrace lze získat na adrese http://www.europen.cz/Akce/6/gnu.pdf

7. DATAKON 2002 -- 1. oznámení o konferenci Databázová konference, 19. - 22. 10. 2002, Hotel SANTON, Brno

Podrobné informace naleznete na http://www.datakon.cz

DATAKON je prestižní česká a slovenská konference s mezinárodní účastí zaměřena na teoretické a technické základy, nejlepší postupy a vývojové trendy v oblasti využití informačních technologií při budování informačních systémů včetně výsledků jejich aplikace v praxi.
DATAKON představuje ideální platformu pro výměnu zkušeností mezi českými i zahraničními odborníky z řad dodavatelů informačních technologií, jejich zákazníků a akademického světa. DATAKON oslovuje zkušené odborníky i nejlepší studenty.

Tématické okruhy
Architektury databázových aplikaci, bezpečnost informačních systémů, datové sklady a OLAP, formální specifikace software, geografické informační systémy, integrace heterogenních informačních zdrojů, Java a databáze, konverze a migrace dat, metadata, ontologie, modelovaní informačních zdrojů v prostředí internetu, multimediální databáze, normy a standardy, objektové relační databáze, jejich modelování a návrh, objevovaní znalosti a data mining, právní aspekty manipulace s informacemi, služby internetu/intranetu a databáze, správa a ladění databází, XML a databáze, workflow, znalostní databáze

Programový výbor DATAKON 2002 (členové viz www.datakon.cz)
Dušan Chlápek, VŠE Praha, předseda

Organizační výbor DATAKON 2001 (členové viz www.datakon.cz)
Jan Staudek, Fakulta informatiky, MU Brno, předseda

Jednací jazyky konference: angličtina, čeština, slovenština

Důležitá data
27.5.2002 - termín podaní návrhu příspěvku
27.6.2002 - oznámení o přijetí/odmítnutí návrhu příspěvku
19.8.2002 - camera-ready forma

Kontaktní adresy
Návrhy příspěvků chlapek@vse.cz
Ostatní komunikace datakon@datakon.cz

Organizují
Česká informatická společnost, pobočka Brno
Česká společnost pro systémovou integraci
Fakulta elektrotechnická, ČVUT Praha
Fakulta elektrotechniky a informatiky, STU Bratislava
Fakulta informatiky, MU Brno
Fakulta informatiky a statistiky, VŠE Praha
Matematicko-fyzikální fakulta, UK Praha
Slovenská informatická společnost

F. Závěrečné informace

1. Sešit

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

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

Pokud se zajímáte pouze o sešit Crypto-World, můžete jej najít na lépe dostupné adrese:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.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@uoou.cz (předmět: ruším odběr Crypto-Worldu !). 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@uoou.cz (**vondruskap@uoou.cz**)

pavel.vondruska@post.cz

vondruska.p@seznam.cz