ČASOVÁ HLEDISKA ELEKTRONICKÉHO PODEPISOVÁNÍ

Miroslav Hrad, Jaroslav Ráček

Fakulta informatiky Masarykovy univerzity, Botanická 68a, 602 00 Brno,
e-mail: xhrad@fi.muni.cz, racek@fi.muni.cz

Abstrakt

Příspěvek se zabývá způsoby připojení časového razítka k elektronickému podpisu. Vedle základních pojmů a principů z oblasti elektronického podepisování, jsou v příspěvku diskutovány i časové aspekty elektronické archivace a z toho plynoucí potřeba časových razítek. Jako základní schémata časového razítka jsou uvedeny jednoduchá, spojovaná a distribuovaná schéma. Dále se příspěvek věnuje absolutním a relativním časovým razítkům. V závěru jsou zmíněny současné autority vydávající časová razítka a je nastíněn možný budoucí vývoj, jež předpokládá i využití jazyka XML.

1. Úvod

Digitální dokumenty se od svých předchůdců v papírové podobě výrazně liší. Přestože obě formy dokumentů umožňují v podstatě stejné typy úkonů jako jsou přenos, archivace, kopírování, opatření podpisem nebo časovým údajem, forma provedení těchto úkonů je u obou typu dokumentů různá. Digitální dokument například může být přenášen či kopírován podstatně vyšší rychlostí, a to bez újmy na jeho kvalitě. Zaznamenat a dokázat jakoukoliv změnu v digitálním dokumentu je však výrazně komplikovanější něž u jeho papírové obdoby. Pokud však chceme považovat digitální podobu dokumentu za dostatečně důvěryhodnou pro bezpečné uchovávání informací, je nezbytné technicky zajistit integritu digitálního dokumentu, a to pro dostatečně dlouhý časový úsek, přičemž toto technické zabezpečení musí být zcela nezávislé na použitém přenosovém médiu.

V současnosti již naprostá většina dokumentů vzniká primárně v digitální podobě a velké množství dokumentů je rovněž digitálně přenášeno veřejnou datovou sítí (internetem). Řada z těchto dokumentů však obsahuje velmi citlivé a hodnotné informace. Je tedy nezbytné zajistit dostatečnou ochranu integrity a nepopiratelnost autorství digitálních dokumentů, což podporují techniky elektronického podpisování.

2. Základní pojmy

Dříve než přistoupíme k popisu jednotlivých bezpečnostních mechanismů, je vhodné zmínit některé základní pojmy z oblasti bezpečnosti IT, s nimiž se v tomto příspěvku pracuje.

Elektronický podpis je technika založená na matematických modelech a teorii složitosti, jež zajišťuje integritu a potvrzuje původce zprávy. Ověření elektronického podpisu je postaveno na principu použití veřejného klíče uvedeného v certifikátu a odpovídajícího privátního klíče pro vytváření podpisů. Elektronickým podpisem ve smyslu zákona č. 227/2000 Sb. o elektronickém podpisu se rozumí údaje v elektronické podobě, které jsou připojeny k datové zprávě nebo jsou s ní logicky spojeny a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Zákon č. 227/2000 Sb. byl přijat v červenci 2000 a nabyl účinnosti 1. října 2000. Zpracovatelé zákona tak zareagovali na novou a v této oblasti zásadní směrnici EU

č. 1999/93 EC o zásadách společenství pro elektronické podpisy, jež byla přijata 13. prosince 1999. Přijatý zákon tak z velké míry vychází z uvedené směrnice EU.

Certifikát veřejného klíče je poskytovatelem vydaná datová zpráva, která slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby a tuto osobu identifikuje. Certifikát spojuje data pro ověřování 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 patří určité osobě. Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby.

Poskytovatel certifikačních služeb (certifikační autorita) je subjekt, jež je důvěryhodný pro uživatele certifikačních služeb, kterým vydává certifikáty, a pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty a zajišťuje jejich správu, včetně vydávání CRL. Certifikační autorita podepisuje svým elektronickým podpisem vydané certifikáty a CRL, čímž je chrání proti případné modifikaci a je identifikovatelná jako subjekt, který je vydal.

CRL - Certificate revocation list je anglický výraz překládaný jako seznam zneplatněných (odvolaných) certifikátů. CRL vydává poskytovatel v pravidelných intervalech. Každý zneplatněný certifikát je v CRL identifikován svým unikátním číslem, které je certifikátu přiděleno při jeho vydání a které je jedinečné u daného poskytovatele. Každý vydaný CRL obsahuje přesný časový údaj svého vydání a je podepsán elektronickým podpisem poskytovatele. CRL je veřejně přístupný, zpravidla se tak děje na webových stránkách poskytovatele. Osoba, která se na podpis spoléhá, tak může do CRL nahlížet, aby zjistila, zda v něm není uvedeno číslo certifikátu, jehož platnost právě ověřuje. Osoba spoléhající se na podpis by rovněž měla svá CRL pravidelně aktualizovat (stahovat si aktuální CRL od certifikačních autorit), neboť starší aplikace toto zpravidla samy nečiní, ani nerozpoznávají, že CRL není aktuální.

3. Elektronický podpis

3.1 Podpis

Zákon rozlišuje dva typy elektronického podpisu, odlišujícího se požadavky, jež podpis musí splňovat. S tím souvisí i právní váha těchto typů podpisu. Prvním typem elektronického podpisu je tzv. *obyčejný elektronický podpis*, jež je definován jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojeny.

Z tohoto pohledu může být obyčejným elektronickým podpisem například k dokumentu připojený naskenovaný podpis, otisk prstu převedený do digitální podoby nebo digitální fotografie.

Druhým typem je *zaručený elektronický podpis*, který musí splňovat následující požadavky:

- Být jednoznačně spojen s podepisující osobou. Toto jednoznačné spojení je v současnosti provedeno nejčastěji prostřednictvím certifikátu nebo kvalifikovaného certifikátu. Podepisující osoba tak nebude moci popřít, že je držitelem soukromého klíče, kterým byl daný dokument podepsán. Z toho pak vyplývá vyvratitelná právní domněnka, že osoba daný dokument podepsala a odeslala.

- Umožňovat identifikaci podepisující osoby ve vztahu k datové zprávě. Jedná se o důvěryhodnost zjištěné identifikace, tedy toho, že osoba je skutečně osobou za kterou se vydává.
- Být vytvořen a připojen k datové zprávě pomocí prostředků, jež podepisující osoba může udržet pod svou výhradní kontrolou Za bezpečnost svých podepisovacích dat plně odpovídá podepisující osoba. Proto je vhodné uschovávat tato data například na disketě či čipové kartě mimo dosah ostatních osob. Pokud jsou tato data uchovávána na počítači, tak by měla být v zašifrované podobě, aby je při případném průniku do počítače nebylo možno získat.
- Být k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. Jedná se zde o integritu zprávy, kdy jakákoliv její modifikace bude rozpoznána. V případě, že by došlo ke změně zprávy, bude příjemce zprávy informován o tom, že došlo ke změně zprávy, nikoli však o tom, co bylo změněno, případně jaká byla původní podoba zprávy.

Elektronický podpis poskytuje identifikaci, tedy zajišťuje:
- totožnost autora - příjemce bezpečně ví, kdo je autorem či odesilatelem podepsaného elektronického dokumentu nebo zprávy.
- integritu obsahu - příjemce má jistotu, že dokument nebyl po podepsání změněn, respektive byl-li změněn, příjemce to zjistí.
- nepopiratelnost zprávy - autor dokumentu nebude moci později popřít své autorství.

Zaručený elektronický podpis je tedy z pohledu zákona stejně důvěryhodný jako například notářem ověřený podpis na papíře.

3.2 Certifikát

Zákon o elektronickém podpisu rozlišuje dva druhy vydávaných certifikátů, jimiž jsou *obyčejný a kvalifikovaný certifikát*. Certifikátem je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost. Spojuje tedy veřejný klíč s podepsanou osobou a potvrzuje identitu této osoby. Tyto certifikáty jsou dnes již běžně vydávány existujícími certifikačními autoritami a na jejich základě jsou elektronicky podepisovány dokumenty.

Kvalifikovaný certifikát je pak certifikát, jež má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávajícím kvalifikované certifikáty.

4. Archivace dokumentů

4.1 Povinnost archivovat

Povinnost archivovat dokumenty je vyžadována různými právními předpisy a týká se jak právnických, tak i fyzických osob. Doba, po kterou je ten který dokument nutno archivovat, se liší. Například český zákon o správě daní a poplatků ukládá povinnost archivovat účetní doklady, které slouží ke stanovení základu daně, a tudíž mohou být předmětem daňové kontroly, v určitých případech až po dobu 18 let. Podklady pro důchodové dávky je nutno uchovávat 25 let. Jiné právní předpisy upravují další lhůty pro uchovávání dokumentů. Jejich zničení dříve, než to příslušný právní předpis dovoluje, je často spojeno s nepříjemnými přímými či nepřímými sankcemi.

4.2 Archivování v elektronické podobě

V současnosti jsou dokumenty ve většině případů archivovány v listinné podobě, což však může zabírat značné prostory. Většinou je tento problém řešen tak, že si firmy najmou externí sklady, kam archivované dokumenty ukládají. Dále praxe ukazuje relativně významné riziko spočívající v tom, že konkrétní dokument dohledávaný v rozsáhlém v listinné podobě vedeném firemním archivu je po několika letech dohledatelný jen velmi obtížně a opět s vynaložením značného času. V případě dohledání požadovaného dokumentu, může být také obtížné doložit pravost obsahu dokumentu, jeho úplnost či neporušenost, může být zpochybňováno datum uvedené na dokumentu či pravost podpisu. Výhodou archivace dokumentů v listinné formě ovšem zůstává, že metodologie pro archivaci je vypracována a pro občany i orgány státní správy je tato srozumitelná.

V době, kdy existuje zákon o elektronickém podpisu a příslušné prováděcí předpisy, se stává technologie elektronického podpisu všeobecně a celosvětově uznávanou a implementovanou. Český zákon o elektronickém podpisu ani související právní předpisy výslovně problematiku elektronické archivace neřeší. Ani v zahraničních právních řádech není tato služba explicitně upravována. To však neznamená, že by archivace elektronických dat a dokumentů byla v rozporu s právními předpisy.

Elektronicky archivovat můžeme v podstatě data libovolného charakteru. Například elektronicky podepsané soubory, emaily, kopie naskenovaných dokumentů, digitalizovaná umělecká díla. Pro archivaci, zvláště pak dlouhodobou, je však často zapotřebí časových razítek.

5. Potřeba časových razítek

Pokud certifikát expiruje (vyprší platnost certifikátu uvedená v certifikátu) nebo byl revokován (byl odvolán - např. z důvodu pochybnosti o důvěryhodnosti privátního klíče), pak je obtížné dostatečně důvěryhodně prokázat, zda byl nebo nebyl odpovídající digitální podpis vytvořen ještě v době platnosti certifikátu či nikoliv. Po tom, co certifikát expiruje, již nikdo nemusí garantovat odpovídající kontrolu nad privátním klíčem. Platnost certifikátu je v současnosti obvykle jeden nebo dva roky. Proto, abychom mohli garantovat bezpečnost digitálních dat jenž jsou digitálně podepsaná i po výrazně delší dobu, je nezbytná další technika, která bude schopná dokázat, že digitální podpis vznikl v době platnosti certifikátu.

Časové razítko je technika dokazující existenci konkrétních digitálních dat ve specifikovaném časovém okamžiku. Metoda časového razítkování digitálních dokumentů musí splňovat alespoň následující dvě vlastnosti:

- Musí se časově orazítkovat data samotná, bez jakékoliv závislosti na použitém médiu, kde se data vyskytují. Jakákoli změna v dokumentu musí být zjistitelná.
- Musí být nemožné orazítkovat dokument časovým údajem odlišným od aktuálního.

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 samotný elektronický podpis, byl vytvořen v okamžiku platnosti jeho certifikátu.

6. Časová razítka - základní schémata

Základní schémata časového razítkování můžeme obecně rozdělit do následujících tří skupin:

- jednoduché schéma (tzv. naivní řešení),
- spojované (linking) schéma,
- distribuované schéma.

Ve všech uvedených schématech se používá pojem *hash* dokumentu. Tím je míněna jednosměrná bezkolizní funkce, která vrací pro libovolný dokument jeho charakteristiku. Charakteristika je vždy stejné délky (předem definované) a je výpočetně obtížné (v praxi nereálné) nalézt pro danou charakteristiku dva rozdílné, této charakteristice odpovídající, dokumenty. Mezi nejznámější a nejpoužívanější hashovací funkce patří MD5 (Message Digest, otisk délky 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů) či nově zaváděná SHA-256 (Secure Hash Algorithm, otisk délky 256 bitů).

6.1 Jednoduché schéma

Jednoduchá schémata (tzv. naivní řešení) nazýváme taková schémata, která pro vytváření časového razítka nevyžadují žádnou informaci z dalších časových razítek či jiných digitálních dat. Scénář vydání takového časového razítka může být následující:

1. Žadatel, jež žádá o vydání časového razítka pro konkrétní data *M*, zašle požadavek obsahující hash dokumentu (hash *H* dokumentu *M*) vydavateli (Time-Stamp Authority - TSA). Přitom je dostatečné zaslat pouze hash dokumentu, dokument nemusí být nikde zveřejněn, ani nemusí putovat veřejnou datovou sítí.
2. Vydavatel časového razítka (TSA) generuje digitální podpis *S* na data, které zahrnují zaslaný hash *H*, časový údaj *T* a vlastní identifikaci *ID*. Časový údaj T obsahuje údaj o okamžiku přijetí žádosti. Výsledné razítko tak obsahuje alespoň *H*, *T*, *ID* a *S*.
3. Vydavatel (TSA) časového razítka zašle vzniklé časové razítko zpět žadateli.

Ověření časového razítka je následující:

1. Ověřovatel vypočítá hodnotu hash dokumentu *M* a porovná s hashem *H* uvedeným v časovém razítku.
2. Ověřovatel ověří platnost elektronického podpisu *S* uvedeného v časovém razítku.

Základní charakteristikou těchto jednoduchých schémat je skutečnost, že celý systém je relativně jednoduchý. Veškerá jeho bezpečnost je však založena na důvěře vůči vydavateli časového razítka. V tomto schématu nic nezabrání případné spolupráci (účelové podvodné dohodě) vydavatele s žadatelem. Nic nebrání vydání razítka neodpovídajícího aktuálnímu reálnému času. Toto nelze ani nijak zpětně detekovat. Právě za účelem řešení problému, že nikdo nemůže detekovat nekorektní vydávání časových razítek, se vyvíjí složitější schémata.

6.2 Spojované schéma

Spojovací schémata lze srovnat s knihou záznamů (například kniha příchodů), kde každý zápis následuje ihned po předchozím a je obtížné provádět posléze úpravy těchto záznamů. Tuto myšlenku poprvé publikovali Haber a Stornetta v roce 1991 [1]. Ve spojovaných schématech vydavatel TSA generuje časová razítka, která obsahují údaje získané z jiných časových razítek (příp. žádostí o časová razítka). Vzniká tak řetěz časových razítek spojovaných některou (předem definovanou) jednosměrnou bezkolizní hashovací funkcí. Kdyby kdokoliv chtěl později pozměnit některé časové razítko nebo vložit zpětně

(antidatovat) do tohoto řetězu jakýkoliv další vstup, musel by pozměnit i celou řadu. To způsobuje při jakékoliv neoprávněné manipulaci s řetězcem časových razítek výrazně náročnější komplikace než u razítek v jednoduchém schématu.

Systémy PKITS a TIMESEC jsou příklady veřejných spojovaných schémat. V systému TIMESEC jsou všechna razítka závislá na všech předchozích razítkách a jsou pravidelně zveřejňována, aby bylo znemožněno vydavateli pozměnit řetěz vznikající z takto vydaných časových razítek. Taková závislost je nutná všude tam, kde nelze zaručit důvěryhodnost TSA. Budování spojovaných schémat je ovšem náročnější než schémat jednoduchých.

6.3 Distribuované schéma

Distribuované schéma je takové schéma, ve kterém více vydavatelů kooperuje na vygenerování časového razítka. Opět, jedním ze základních cílů tohoto schématu je posílení bezpečnosti, tj. omezení možností vydavateli manipulovat s časovými razítky. To se zabezpečuje sdílením tajných dat pro vytváření časových razítek mezi více vydavateli. Jestliže je počet ve shodě kooperujících vydavatelů menší než nějaký předem definovaný počet, je nemožné dát tato tajná - nezbytná data dohromady a není tedy možné razítko vydat. Budování distribuovaných schémat, obdobně jako spojovaných schémat, je ovšem náročnější než schémat jednoduchých.

7. Absolutní a relativní časová razítka

7.1 Absolutní časová razítka

Absolutní časová razítka (podepsaný hash) jsou značky (podepsané TSA), které spojují dokument (resp. hash dokumentu) s časovým okamžikem reprezentovaným jako číslo. Bezpečnost tohoto systému je založena na předpokladech, že TSA má přesný čas (zařízení udávající přesný čas) a je zcela důvěryhodná.

7.2 Relativní časová razítka

Nechť h je bezkolizní jednosměrná hashovací funkce a x, y jsou dva bitové řetězce o nichž víme, že, $y = h(x)$ a y byl zveřejněn k datu D (tj. existoval k datu D). Pak z důvodu jednosměrnosti funkce h můžeme dokázat, že x byl znám dříve, než byl někým vytvořen y, tedy můžeme s jistotou tvrdit, že x byl vytvořen před datem D. Danou situaci můžeme dále zobecnit do tvaru

$$y = h(x_1, x_2, \ldots, x_n) \quad . \tag{1}$$

Nechť $y = Sig_A\{X\}$ je subjektem A podepsaný dokument X a $\sigma = Sig_B\{Y, y\}$ je subjektem B podepsaná zpráva Y , která zahrnuje i bitový řetězec y. Pak $(x_1, \ldots, x_n)$ je nezpochybnitelný důkaz, že subjekt A podepsal dokument X před tím než subjekt B podepsal Y. Tento důkaz není založen na klíčové kryptologii a vychází pouze z vlastností jednosměrné bezkolizní hashovací funkce. Průkaznost tudíž není ohrožena problémem s kompromitací klíče.

7.3 Průkaznost časových razítek

TSA průběžně vytváří a udržuje *secure log*, což je tzv. *bezpečnostní záznam* $(l_0, l_1, \ldots, l_n, \ldots)$. Tento secure log je opět založen na využití bezkolizní jednosměrné

hashovací funkce (např. h) s k-bitovým výstupem. Při přijetí každého požadavku o časové razítko x_n TSA vypočítá novou hodnotu l_n užitím následující rekurzivní formule:

$$l_n = h(x_n , l_{n-1}) \quad (2)$$

Nejdůležitější vlastností tohoto spojovaného schématu je, že hodnota každé položky l_n v secure log závisí na chování jednosměrné funkce na předchozích položkách $l_0, \ldots, l_{n-1}$. Jestliže l_n již byla v den D zveřejněna, tak:

- předchozí hodnoty nemohou být změněny bez možnosti detekce auditorem,
- záznam $(l_0, \ldots, l_n)$ z secure log může být použit jako důkaz existence pro $x_0, \ldots, x_n$ před dnem D.

Čas od času publikuje TSA poslední dosažené l_n. Například společnost Surety pravidelně zveřejňuje poslední dosažený secure log v nedělním vydání New York Times. Po tomto zveřejnění ani TSA, ani nikdo jiný není schopen modifikovat řetěz $l_0, \ldots, l_{n-1}$ předchozích záznamů v secure log. Pro prokázání pořadí l_m a l_n (kde $m < n$) potřebuje ověřovatel získat seznam $T_{m,n} = (x_{m+1}, x_{m+2}, \ldots, x_n)$ a provést $n - m$ kroků (výpočtů hashovací funkce). Seznam $T_{m,n}$ je pak nezpochybnitelný důkaz, že l_m bylo vydáno před l_n.

7.4 Čerstvost

Potřebujeme-li zaručit, že zpráva Z byla podepsána až po čase t, můžeme použít schématu, kdy žadatel A pošle požadavek na TSA. Tato TSA podepíše aktuální čas t a pošle $H = Sig_{TSA}\{t\}$ zpět žadateli A. Žadatel A pak připojí ke zprávě Z potvrzený časový údaj H a vše následně podepíše svým elektronickým podpisem. Pro takto vzniklou zprávu $\sigma = Sig_A\{Z, H\}$ je ověřovatel B schopen ověřit, že zpráva Z byla podepsána až po čase t uvedeném v H.

7.5 Časový interval

Chceme-li prokázat, že zpráva Z byla podepsána v daném časovém intervalu $[t_1, t_2]$, je nejdříve zapotřebí, aby si žadatel A vyžádal od TSA podepsaný časový údaj $H = Sig_{TSA}\{t_1\}$ a následně vytvoří $\sigma = Sig_A\{Z, H\}$, čímž potvrdí čerstvost podpisu. Poté žadatel A odešle zprávu σ (resp. její hash) na TSA. Tato TSA připojí aktuální datum a čas t_2 ke zprávě σ a zašle $T = Sig_{TSA}\{\sigma, t_2\}$ zpět žadateli A. Vzniklá trojice (H, σ, T) je důkazem, že A podepsal Z v časovém intervalu $[t_1, t_2]$.

Je zřejmě nemožné určit přesný moment vzniku podpisu třetí stranou. Můžeme však zjistit dva momenty - jeden před (t_1) a druhý po (t_2) vytvoření podpisu. S využitím těchto dvou časových značek můžeme později dokázat, že podpis byl vytvořen v průběhu daného časového intervalu.

8. Autorita vydávající časová razítka

RFC 3161 (Request for Comments 3161) definuje Time-Stamp Protocol (protokol pro časová razítka). Tento dokument popisuje formát žádostí zasílaných na TSA (Time Stamping Authority - autorita vydávající časová razítka) a formát odpovědí jenž má TSA vracet.

8.1 RFC 3161

TSA je definována jako TTP (Trusted Third Party - důvěryhodná třetí strana), která vytváří časová razítka pro důkaz existence dat v daném časovém okamžiku.

8.1.1 Požadavky na TSA

Na TSA odpovídající RFC 3161 jsou kladeny následující požadavky:

- používat důvěryhodný zdroj času,
- vkládat důvěryhodnou časovou hodnotu do každého časového razítka,
- každé nové časové razítko generovat s jedinečným sériovým číslem,
- pokud je to možné, vytvářet časové razítko pro každou správnou žádost,
- do každého časového razítka vložit identifikaci bezpečnostní politiky,
- označovat časovým razítkem pouze hash reprezentace dat, tedy výsledky jednocestných hashovacích funkcí jednoznačně identifikovatelných pomocí OID (identifikátoru hashovacího algoritmu),
- kontrolovat, že délka hashe odpovídá definované délce jednocestné hashovací funkce identifikované pomocí OID,
- netestovat jiným způsobem korektnost OID,
- nezahrnovat identifikaci žadatele do časového razítka,
- podepisovat každé časové razítko klíčem a certifikátem využívaným výhradně pro tyto účely,
- odpovídat chybovým hlášením, pokud jsou požadovány doplňkové informace, které TSA neposkytuje.

8.1.2 Politika TSA

Politika TSA by měla definovat nejméně tyto typy informací:

- podmínky za kterých může být užito časové razítko,
- dostupnost logu (záznamů) časových razítek pro umožnění pozdější kontroly pravosti.

8.1.3 Časový údaj

Časový údaj uvedený v časovém razítku reprezentuje moment vytvoření razítka TSA. Údaj je podle RFC 3161 vyjádřen jako čas UTC (Coordinated Universal Time), aby se předešlo problematice časových zón (Greenwich Mean Time). Tento údaj je synonymem k času "Zulu", jež se používá v civilním letectví. Přesnost nejméně jedné sekundy je zajištěna syntaxí zápisu YYYYMMDDhhmmss[.s....]Z. Zápis 20030101000000.001Z tedy například reprezentuje čas odpovídající přesně jedné tisícině sekundy po počátku roku 2003.

8.1.4 Transportní protokoly

RFC 3161 jsou uvádí následující transportní protokoly:

- protokol užívající e-mail. Žádost o razítko (resp. odpověď) je definována jako MIME objekt následovně:

  Content-Type: application/timestamp-query ,
  Content-Type: application/timestamp-reply .

- protokol založený na souborech. Jedná se o soubory s příponou .tsq (Time-Stamp Query) a .tsr (Time-Stamp Reply).
- komunikace sockety přes IP port číslo 318.
- protokol založený na HTTP (Hyper Text Transfer Protocol). Žádost o razítko (resp. odpověď) je definována jako MIME objekt následovně:

  Content-Type: application/timestamp-query ,
  Content-Type: application/timestamp-reply .

9. Možný vývoj

Další možnosti vývoje v této oblasti spatřují autoři příspěvku především ve využitím jazyka XML (eXtensible Markup Language), přičemž lze očekávat, že dojde k integraci prostředků elektronického podepisování a časových razítek.*XML Signature* je metoda umožňující spojení veřejného klíče, podpisu a podepisovaných data. Nezabývá se přitom způsobem, jakým je spojen veřejný klíč s podepisující osobou, ani smyslem podepisovaných dat. Podepsat lze jak dokument XML, tak jakýkoli jiný dokument. *XML Advanced Electronic Signatures* je rozšíření XML signature, které již zahrnuje i možné zakomponování časových razítek.

Elektronická komunikace založená na výše zmíněných principech již nyní významně zjednodušuje a urychluje práci a není pochyb, že časová razítka se stejně jako elektronický podpis stanou významným prvkem této sféry. Širšímu využití časových razítek však budou muset vedle mnoha technologických kroků předcházet rovněž legislativní úpravy. Současný český právní systém používání časových razítkek vůbec neřeší. Se vstupem České republiky do Evropské unie však můžeme i v této oblasti očekávat změny.

Reference:

1. Bosakova, D., Hobza, J., Stachovcova, L., Vondruska, P.: Elektronický podpis od A do Z, http://www.mvcr.cz/casopisy/s/2002/0040/pril.html, 2002.
2. Haber, S., Stornetta, W.: How to time-stamp a digital document, Journal of Cryptology, 3(2):99-111, 1991.
3. Hodkova, I.: Archivační autorita – archivace elektronických dokumentů s certifikací, http://www.landwellglobal.com/cz/cze/insights/archivacniautorita cz.html, 2002.
4. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, http://www.ietf.org/rfc/rfc3161.txt