Dokumenty a jejich věrohodnost

1 Listinné (analogové) dokumenty

Listinné dokumenty jsou dosud nejčastější a zdánlivě nejbezproblémovější dokumenty, jaké se používají. Listinný dokument je vytištěn na zpravidla bílém papíru a obvykle opatřen značkou věrohodnosti. Značka věrohodnosti může být:

- **Razítko**

  a/nebo

- **Podpis**

Razítko představuje otisk textu, často doplněný grafikou vytvořený zařízením pro opakované použití. Význam razítka jako značky věrohodnosti dokumentu klesl jednak snížením dostupnosti razítek, usnadněním možností jejich napodobení a zejména interakcí s mezinárodní praxí, v níž není závazné užití razítek povinné. V minulých dobách bylo významným faktorem věrohodnosti dokumentů označených razítky to, že otisky razítek musely být závazně evidovány právě tak jako jejich vlastnictví.

> *Jedinou známou výjimkou je dle naší legislativy (zejména Správní řád) je použití kulatých razítek se státním znakem na rozsudcích a správních rozhodnutích, kdy razítko symbolizuje, čí jménem bylo rozhodnutí nebo rozsudek učiněno.*

Podpis je ve světě uznávaná značka věrohodnosti a je to ruční grafický útvar vycházející z příjmení případně i jména podepisujícího, kdy mnohem více než čitelnost má význam unikátní grafická podoba. Faktorem věrohodnosti je obtížná napodobitelnost, vycházející z unikátních vlastností lidské motoriky.

Podpisy bývají obvykle barevně odlišeny, typicky modrou barvou od textu, k němuž se vztahují.

Důležité je, že aniž by to bylo explicitně v legislativě uvedeno, musí být z textu a obsahu dokumentu, k němuž se listinný podpis vztahuje, jasně patrné, co vlastně připojený podpis znamená. Zpravidla je to: **Autorství a zodpovědnost**.

> ✓ U listinných dokumentů se automaticky předpokládá, že z jejich obsahu lze dovodit **důvod podpisu**.

> *Předchozí závěr platí i pro takové dokumenty, které obsahují více podpisů. Někdy nazývaných **parafy**.*

> *Historicky byla značkou věrohodnosti i Pečeť. Její význam dnes je zanedbatelný, právě tak jako význam jiných archaických typů značek.*

2 Digitální dokumenty

Digitálními dokumenty rozumíme dokumenty vedené v digitální podobě. V této podobě jsou dokumenty v originále.

> *Jako dokument vedený digitálně nelze rozhodně považovat prostý sken papírového originálu, který často umožňují systémy elektronické spisové služby (ESS). V takových případech se jedná jen o technické pomůcky pro usnadnění práce uživatelů.*

2.1 Soubory ve zdrojovém tvaru

Soubory ve zdrojovém tvaru jsou typicky výstupy z programů/aplikací, které umožňují takové soubory plnohodnotně modifikovat. Nejtypičtějšími představiteli takových souborů jsou výstupy textových editorů (MS Word). Patří sem ale i jiné, byť méně používané aplikace pro tvorbu CAD, mapové i jiné dokumentace. U těchto dokumentů pro jejich archivační účely lze identifikovat dva okruhy problémů:

- Jejich formát je zpravidla firemní, absentuje zde proto záruka dlouhodobé čitelnosti a zobrazitelnosti v neměnné vizuální podobě.
- Absentuje jasný a mezinárodně uznaný formát digitálních značek.

> *To je také důvod, proč bývají tyto soubory konvertovány pro účely dlouhodobého uložení do jiných formátů, které jsou popsány dále.*

2.2 PDF dokumenty

Dokumenty ve formátu .PDF jsou základem pro dlouhodobé uložení. Historicky se jedná o ryze firemní formát firmy Adobe Inc. ® Definice formátu se vyvíjela, ale původní idea byla taková, že dokument ve formátu .PDF by měl být zobrazitelný i vytisknutelný v neměnné vizuální podobě bez ohledu na platformu, operační systém apod. Postupně firma Adobe Inc. ® definici formátu rozšiřovala, například o možnost použít soubor .PDF jako obálku pro úschovu jiných libovolných souborů apod. , čímž se postupně vytratil původní účel formátu .PDF.

Každopádně se formát souboru . PDF stal rovněž ISO normou, čímž se z oblasti komerčních firemních standardů posunul do oblasti použitelné v legislativě.

> *Problém ale zůstal v tom, že norma .PDF byla paradoxně příliš bohatá na to, aby mohla být použita pro dlouhodobé uložení, neboť její formát nezaručoval úplnou a neměnnou zobrazitelnost nezávisle na platformě.*

2.3 PDF/A dokumenty

Definice PDF/A se tedy naoko vrátila zpátky v čase a výrazně omezila možnosti formátu. Soubory mají i nadále příponu .PDF. Definice .PDF/A podstatně zpřísňuje podmínky. Nesmí obsahovat žádné odkazy mimo soubor, musí mít všechny potřebné fonty, nesmí obsahovat, krátce řečeno, žádnou informaci, která by nebyla jasně a jednoznačně zobrazitelná. Jinými slovy musí obsahovat pouze a jen to, co má být zobrazeno.

> *Pozornější čtenář by mohl položit všetečnou otázku, jak se toto pravidlo srovnává s existencí vnitřních digitálních podpisů dokumentů PDF/A (jsou to tedy ještě vůbec dokumenty PDF/A? Jsou neboť společnost Adobe Inc. ® to vyřešila s moudrostí politiků: udělala výjimku.*

2.4 Uložení a vlastnosti

2.4.1 Digitální podpis

Dokumenty v PDF/A (nakonec i v PDF obecně) mohou obsahovat jeden digitální podpis nebo i podpisů více. Dokument .PDF/A obsahující digitální podpis se skládá z původního dokumentu bez podpisu, k němu přidaného podpisu a to je celé zabaleno v celkovém dokumentu.

> *Z toho vyplývá, že i kdyby jeden člověk chtěl jedním podpisovým certifikátem jeden dokument podepsat vícekrát, bude každý podpis jiný, resp.pokaždé se dokument změní.*

Důležité je uvědomit si přesně, co znamená takový digitální podpis na dokumentu:

Říká pouze a právě jen to, že dokument podepsala osoba vlastnící certifikát, který byl v okamžiku podpisu platný. Nic víc a nic míň. Samotný podpis (digitální) neříká nic o zodpovědnosti za obsah dokumentu. Samotný důvod připojení digitálního podpisu by měl být patrný z obsahu dokumentu, jinak může dojít k významným nedorozuměním.

> *Tato zásada je bohužel v reálné praxi masivně porušována. Jakožto odstrašující příklad může sloužit bohužel nikoli řídká praxe u mnohých orgánů veřejné moci, kdy podatelna podepíše došlý digitální soubor v .PDF bez dalšího svým podpisem. Tím se chová tak, jako by za něj sama převzala totální zodpovědnost.*

✓ Na digitálně vedeném dokumentu by měl být vždy jasný odkaz na připojený digitální podpis s uvedením důvodu podpisu.

Zvláštním případem je tzv. vizualizovaný podpis. Je to plnohodnotný digitální podpis, který se na vizuální podobě dokumentu zobrazuje obdobně jako naskenovaný ruční podpis. Je to dobré jak pro méně technicky zdatné uživatele, tak to umožňuje lépe a názorněji vpravit do obsahu dokumentu odkaz na podpis a jeho důvod.

2.4.2 Časové razítko

Časové razítko se vytváří tak, že se vytvoří hash dokumentu, k němu se přiřadí normalizovaný časový údaj a to celé podepíše autorita časových razítek svým digitálním podpisem.

> *Z výše uvedeného vyplývá, že „orazítkovat" lze dokument jakéhokoliv typu, tedy nejen .PDF/A.*

✓ Časové razítko tedy (je-li platné) říká právě jen to, že předmětný řetězec bytů určitě existoval v daném okamžiku někde na internetu.

2.4.3 Věrohodnost dokumentů a PKI značky

PKI značkami rozumíme podpisy, systémové značky a časová razítka, tedy je založeno na asymetrické kryptografii.

Dokument s digitálním podpisem

Jeho podpis musí být platný. Platný je právě tehdy, je-li platný podpisový certifikát, jímž byl podpis vytvořen. Pokud je certifikát

revokován nebo prostě expiruje, pak je takový dokument zcela neprůkazný.

- *I zde ale platí zásada, že obsah dokumentu by měl aspoň implicitně odkázat na připojený podpis s uvedením, co podpis znamená.*

Dokument s digitálním podpisem a časovým razítkem

Pokud jsou zároveň splněny podmínky paragrafu 69a, pak je takový dokument z pohledu legislativy považován za „pravý". Ty podmínky jsou zejména ty, že podpis musel být uznávaný a platný v době podpisu a razítko uznávané.

- *Zde je podstatné uvědomit si, že časové razítko (uznávané i neuznávané) je technickou podstatou digitálním podpisem, tudíž musí dříve či později expirovat. Naše legislativa v platném znění považuje takto označené dokumenty za „pravé", i když razítko již dávno expirovalo. To v sobě skrývá úskalí, že pokud příslušné ustanovení zákona přestane z jakýchkoliv důvodů platit, všechny dokumenty označené „expirovaným" razítkem budou nevratně právně nerelevantní!*

Dokument s digitálním podpisem a opakovaným časovým razítkem

Pokud je dokument připraven na počátku svého životního cyklu podle předchozího odstavce, pak před uplynutím expirační doby prvního razítka lze dokument „přerazítkovat". Tím se odstraní výše zmíněná závislost na legislativě a dokument by měl být považován za „pravý" i v případě, že paragraf 69a přestane platit. Pravost takového dokumentu pak musí být povrzena jakýmkoliv objektivním soudním znalcem v případě potřeby.

- *Problémem zde je, že každý otisk časového razítka je zpoplatněn, tudíž takto udržovat velké množství dokumentů se tak může nemálo prodražit.*

Dlouhodobý důvěryhodný archív

Uložení dokumentů s obnovováním razítek zaručuje jejich technickou i právní relevanci bez ohledu na stav legislativy, má tedy i mezinárodní dopad.

Aby se uživatelé vyhnuli neúnosně velkým nákladů na přerazítkování, byly vyvinuty algoritmy, kdy se přerazítkovávají zjednodušeně řečeno skupiny dokumentů, čímž je jejich pravost jištěna hromadně. Jedním z nejznámějších algoritmů je vytváření tzv Merkleových stromů. Jejich význam spočívá v tom, že trvale zaručuje relevanci dokumentů a výrazně šetří náklady na obnovu razítek (až několikanásobně).

- *Z uvedeného jasně vyplývá, že dlouhodobá důvěryhodnost z obsahového hlediska nijak nezávisí na vlastnostech použitého HW.*

2.4.4 Další požadavky na dlouhodobou důvěryhodnost

Neměnnost

Je z pohledu legislativy zajištěna použitím razítek. Tento pohled má mezinárodní platnost.

- *Je třeba upozornit na úskalí, že pokud dojde k diskreditaci klíče TSA, pak jsou zneplatněna veškerá její razítka zpětně! Proto lze vřele doporučit používat paralelně více TSA tak, aby řetězec důvěryhodnosti nebyl při diskreditaci jednoho jejich klíče znehodnocen. V katastrofickém případě (diskreditace klíče TSA) musí být k dispozici procedura náhrady diskreditovaného klíče klíčem jiné TSA.*

Stálost

Toto je vlastnost, kterou lze podpořit vyspělými HW technologiemi a technologiemi typu Mirror, Cluster apod.

Dlouhodobá čitelnost a zobrazitelnost

Tato důležitá vlastnost je zajištěna mezinárodní certifikací formátu souborů, typicky PDF/A.

3 Úloha pokročilých HW prostředků

WORM

Prostředky WORM (Write Once Read Many) zajišťují neměnnost záznamu na nich. Nejsou odolné proti fyzickému zničení a samy o sobě neobsahují žádné prostředky prokazatelnosti obsahu.

Disky CAS

Prostředky CAS (Content Addressable Storage) bývají často považovány za samospasitelné zajištění průkaznosti jejich obsahu.

Přinášejí uživatelům řadu výhod, ale základní faktory prokazatelnosti obsahu v sobě nemají. Ty musí být zajištěny jinak. Deklarovaná nesmazatelnost a WORM vlastnost je nepochybně užitečná, nicméně sebedokonalejší HW úložiště není odolné vůči fyzickému zničení. Tudíž i zde musí být nějak zajištěna funkce zálohy.

4 Historie verzí

Verze	Datum	Obsah	Autor
1.0	28.10.2012	První verze	Vladislav Krásný

V Plzni, dne 28.10.2012 Vladislav Krásný