Důvěryhodný digitální dokument

Stanovisko ICT UNIE k problematice právně validního dokumentu

Poziční dokument ICT UNIE

ICTU 2014

Obsah

1 Manažerský souhrn 3

2 Terminologie 5

3 Úvod 11

4 Důvěryhodný dokument 12

5 Služby pro vznik a zachování důvěryhodnosti dokumentu 15

6 Důkazní materiál 16

7 Analýza způsobů ztráty důvěryhodnosti 17

8 Navazující aktivity pracovní skupiny ICTU – Archivnictví 24

9 Závěr 26

Seznam obrázků:

Obrázek 1: Osa životního cyklu dokumentu 11

Obrázek 2: Způsob vyhodnocení důvěryhodnosti dokumentu 17

Obrázek 3: Vztah technické a logické podoby dokumentu 18

Obrázek 4: Vytvoření a ověření elektronického podpisu 20

1 MANAŽERSKÝ SOUHRN

V České republice dlouhodobě chybí jednoznačná definice důvěryhodného elektronického dokumentu a jasná pravidla, jak s tímto dokumentem zacházet, aniž by ztratil svoji důvěryhodnost. Narůstající množství dokumentů v elektronické podobě, které nejsou udržovány v důvěryhodném stavu, může totiž v budoucnosti přinášet právní nejistotu a zapříčinit složité spory. Proto se pracovní skupina Archivnictví ICT UNIE rozhodla v loňském roce na tuto potřebu reagovat.

Prvním výsledkem je dokument, který definuje parametry „důvěryhodného digitálního dokumentu“ tak, aby splňoval jak legislativní, tak i bezpečnostně-technické požadavky. Kromě toho vyjmenovává služby, které jsou nezbytné pro efektivní zafixování, údržbu a používání důvěryhodných dokumentů.

Tento dokument je první z řady dokumentů, které se zabývají elektronickým dokumentem v rámci jeho celého životního cyklu, od jeho fixace do důvěryhodné podoby až po jeho zničení.

Definice důvěryhodného digitálního dokumentu

Dokument[1] je důvěryhodný, pokud jsou splněny následující požadavky:

- Jedná se o originální (autentický, původní) dokument nebo jeho odvození z originálního dokumentu (např. stejnopis či jeho konvertovanou verzi).
- Lze jednoznačně určit původ dokumentu.
- Lze jednoznačně ověřit, že nedošlo k porušení integrity dokumentu[2].
- V případě kopie, repliky nebo konverze lze doložit shodu s originálem.
- Je zaručena jeho čitelnost.
- Lze jednoznačně prokázat existenci dokumentu v čase.

Dokument ztrácí svou důvěryhodnost zejména tehdy:

- je-li nečitelný;
- došlo-li k porušení jeho integrity;
- není-li možno jednoznačně prokázat platnost bezpečnostních prvků zaručujících jeho důvěryhodnost (elektronický podpis, časové razítko, hashovací algoritmus) v době jeho vzniku.

Další výstupy práce na dokumentu

1. Součástí dokumentu je analýza způsobů ztráty důvěryhodnosti digitálního dokumentu. Jejím cílem je pomoci pochopit, na jakých principech je konstrukt „důvěryhodnosti“ či „pravosti“ vystavěn, pomocí jakých prostředků jsou tyto principy prosazovány, jaká jsou jejich inherentní omezení a jak lze tato omezení překonat.
2. Pracovní skupina v rámci práce na tomto dokumentu identifikovala řadu problémů, které je nutné v souvislosti s dalším zaváděním digitálních dokumentů do praxe řešit.

1 Důvěryhodný dokument je právně nezpochybnitelný. Neměnnost a neporušitelnost dokumentu lze obtížně zaručit, pouze lze činit opatření, která to znesnadňují. Místo toho lze požadovat jednoznačnou detekovatelnost porušení integrity dokumentu.
2 Definice důvěryhodného dokumentu obsahuje požadavek na porušitelnost integrity dokumentu, který zahrnuje i případnou změnu dokumentu dynamickými prvky.

Mezi nejvýraznější problémy patří následující:

- Neexistence jasných a společných pravidel, jak postupovat při komunikaci a ukládání důvěryhodných digitálních dokumentů mezi subjekty veřejné moci a komerční sférou a při komunikaci mezi komerčními subjekty např. při obchodním styku.

  Tato pravidla jsou v současnosti stanovena hlavně pro státní správu a samosprávu a komerční sféry se dotýkají pouze okrajově. Kromě toho jsou ze strany státní správy vůči komerčním subjektům nejednotně vykládána.

- Neexistence registru elektronických identit osob, který by byl všeobecně dostupný pro ověření dané osoby jak pro státní správu a samosprávu, tak i pro komerční sféru i samotné občany. S tím je spojena také problematika elektronického identifikačního dokladu, která v České republice zůstala nedořešena.
- Fikce elektronického podpisu zpráv odeslaných datovou schránkou, zavedená zákonem o elektronických úkonech a autorizované konverzi dokumentů.
- Rozpor mezi občanským zákoníkem a zákonem o elektronickém podpisu v oblasti nahrazení elektronického podpisu elektronickou značkou.
- Neexistence či pomalý rozvoj služeb určených pro vznik a zachování důvěryhodnosti digitálního dokumentu.
- Konverze dokumentů. Jedná se o celý balík problémů, který trápí jak občany, tak i komerční sféru. Příkladem může být omezený rozsah služby autorizované konverze pouze na formát PDF nebo její cena při konverzi velkého počtu dokumentů.

Předpokládaný vývoj

Pracovní skupina si je vědoma, že pouhá definice „důvěryhodného digitálního dokumentu“ není dostačující. Z tohoto důvodu na konci roku 2013 vznikly nové pracovní týmy, které pracují na definici pravidel pro komunikaci, správu a dlouhodobé ukládání důvěryhodného digitálního dokumentu a formátu jeho „důkazního materiálu“ prokazujícího, že důvěryhodnost dokumentu nebyla narušena. Jejich výstupy by měly s tímto dokumentem tvořit ucelený koncept.

Následně bude tento koncept ze strany ICT UNIE veřejně popularizován.

Zároveň se bude ICT UNIE aktivně podílet na zavádění připravovaných opatření Evropské komise v oblasti důvěryhodných služeb a podpoří vznik efektivní infrastruktury v této důležité oblasti.

2 TERMINOLOGIE

Termín	Význam
AdES	Advanced Electronic Signature (Direktiva EU 1999/93/EC) – skupina standardů definujících podobu rozšířených elektronických podpisů (CAdES, XAdES, PAdES).
Archivní balíček	Archival Information Package (nebo také AIP) je definovaný normou ISO 14721:2012 – Open Archival Information System (nebo také OAIS). Jedná se o dokument(y) a jeho metadata, zabalené do XML obálky.
Autentický	Původní, pravý.
Bezpečnostní prvek	Elektronický podpis, elektronická značka, časové razítko (a jejich kvalifikované certifikáty), CRL listy, validační zpráva a OCSP protokol.
Certifikát	Certifikátem se rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.
CRL	Certificate revocation list – seznam zneplatněných certifikátů vydaný a podepsaný certifikační autoritou.
Časové razítko (kvalifikované)	Kvalifikovaným časovým razítkem se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.
Čitelnost	Čitelností elektronického dokumentu rozumíme možnost získat datový obsah uložený v dokumentu. Dokument uložený jako elektronický nebo jiný záznam v analogové nebo digitální formě není přímo čitelný člověkem, ale vyžaduje technické a případně i softwarové prostředky pro čtení nebo vizualizaci.
Datová zpráva	Jedná se o elektronická data, která lze přenášet prostředky pro elektronickou komunikaci (např. informační systém datových schránek) a uchovávat na technických nosičích dat používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru.
Digitální dokument	Digitálním dokumentem se rozumí dokument v elektronické podobě; viz také elektronický dokument.

Termín	Význam
Dokument	Podle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové, či digitální, která byla vytvořena původcem nebo byla původci doručena. Dokument má tedy obecnější podobu než písemnost, neboť předpokládá více forem než pouze písemnou. Podle platné právní úpravy musí být právní úkon podepsán jednající osobou vlastnoručně. V případech, kdy je to obvyklé, může být nahrazen mechanickými prostředky (např. razítkem). Je-li právní úkon učiněn elektronicky, může být podepsán zaručeným elektronickým podpisem.
Doručování	Různé způsoby odesílání a poskytování dokumentů: zasílání prostřednictvím odesílajících a přijímajících subjektů, zasílání konzulární nebo diplomatickou cestou, prostřednictvím poštovních služeb a přímým doručením. Odesílající subjekty odpovídají za odesílání soudních a mimosoudních dokumentů doručovaných do jiného členského státu. Přijímající subjekty odpovídají za příjem soudních a mimosoudních dokumentů z jiného členského státu. Ústřední orgán poskytuje informace odesílajícím subjektům a hledá řešení veškerých obtíží, které mohou vzniknout při zasílání písemností určených k doručení.[3]
Důvěra	Důvěra je spolehnutí se na něco, očekávání něčeho, je určující faktor v procesu rozhodování. Znamená vztah spoléhání na druhé lidi, instituce nebo věci.
Důvěryhodnost	Důvěryhodnost je vlastnost vztažená k nabízené nebo poskytované službě, ze které je možno odvodit důvěru v řádné provedení této služby.
Elektronická značka	Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.
Elektronický dokument	Elektronickým dokumentem se rozumí dokument v elektronické podobě

3 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007R1393:CS:NOT

Termín	Význam
Elektronický podpis	Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.
Fixace	Stav dokumentu, ve kterém je daný dokument již nadále obsahově neměnný.
Integrita dokumentu	Integritou rozumíme neporušenost původního dokumentu, zejména skutečnost, že nedošlo k neoprávněné změně informace obsažené v dokumentu.
Kolizní situace	Jedná se o stav, kdy daný dokument nesplňuje kritéria pro dokončení fáze karantény (např. neúplná povinná metadata). Tento stav vyžaduje zásah správce archivu, který stav napraví nebo rozhodne o dalším postupu, viz NSESSS, kap. 2.2. Matice příkladů rolí v rámci ERMS.
Kontextuální odkaz	Odkaz na dokument, který je s daným dokumentem v určitém obsahovém nebo logickém vztahu.
Kvalifikovaný certifikát	Kvalifikovaným certifikátem se rozumí certifikát, který má náležitosti podle § 12 zák. č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a byl vydán kvalifikovaným poskytovatelem certifikačních služeb.
Listina	České právo nedefinuje, jakým materiálem je listina tvořena. Obecně se má za to, že listinou je papír nebo jakýkoli jiný hmotný substrát, na němž lze zachytit písemný obsah. Za listiny po roce 1850 se pro účely evidence archiválií jako jednotliviny nepovažují dokumenty zakládající právní akty uvedené v primárních registrech, jmenování čestným občanem, výuční listy, osobní doklady, školní vysvědčení, diplomy, statuty a stanovy spolků. Jako listiny se rovněž neevidují a nevykazují cenné papíry. Jako listiny po roce 1850 se neevidují listiny, které jsou součástí spisů.[4]
Metadata	Data popisující kontext, obsah a strukturu dokumentů nebo jiných entit a jejich spravování v čase. Povinná metadata je nutné vyplnit vždy, protože podléhají automatické kontrole na vstupu do systému. Nepovinná metadata kontrolována nejsou.

4 Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů v platném znění.

TERMINOLOGIE

Termín	Význam
Omezení rozsahu důvěryhodnosti	Každý dokument prochází určitým životním cyklem, od svého vzniku, používání, autorizované změny po archivaci, skartaci. Pro účely tohoto dokumentu je rozhodující okamžik, kdy jsou zafixovány všechny 4 požadavky na důvěryhodný dokument, zpravidla při jeho uložení do systému pro správu důvěryhodných dokumentů. V zákoně č. 499/2004 Sb. je zakotvena právní domněnka pravosti dokumentů, což je z mnoha důvodů nebezpečná konstrukce.
Písemná forma právních jednání (písemnost)	§ 562 zákona č. 89/2012 Sb., občanský zákoník: Odst. 1: Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Odst. 2: Má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý. (Pozn.: Účinnost od 1. ledna 2014.)
Původce	Původcem je každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán.
Původ dokumentu	Původem dokumentu rozumíme identifikaci entity, z jejíž činnosti dokument vznikl, a další atributy, které umožňují jednoznačně identifikovat dokument v kontextu jeho vzniku nebo přijetí.
Replika digitálního dokumentu	Replikou se pro účely péče o archiválii v digitální podobě rozumí řetězec znaků totožný s dokumentem v digitální podobě, z něhož byl vytvořen.
Relevantní výběr	Splňuje určitou míru shody mezi zadaným klíčem (vyhledávacími údaji) a nalezenou referencí (seznamem relevantních dokumentů).
SIP	Submission Information Package – informační objekt vstupující do archivu ze zdrojového systému (na počátku archivačního životního cyklu dokumentu) dle definice OAIS. Součástí SIP balíčku je jeden nebo více dokumentů a jejich metadata.
Skartační řízení	Skartačním řízením se rozumí proces vyřazování dokumentu z fondu organizace, který se řídí skartačním režimem.

Termín	Význam
Skartační návrh	Skartačním návrhem se rozumí návrh organizace na výběr a vyřazení archiválií a skartaci dokumentů s uplynulou skartační lhůtou, které nejsou nadále provozně nebo správně potřebné. Součástí skartačního návrhu je seznam dokumentů typu „A“ (tzv. archiválie) a seznam dokumentů s uplynulou skartační lhůtou se skartačními znaky S a V. Skartační návrh může být předkládán k posouzení a schválení věcně a místně příslušnému státnímu archivu pověřenému dohledem na výběr archiválií a vyřazování dokumentů organizace navrhovaných ke skartaci.
Skartační režim	NSESSS[5]: Skartační režim je organizací stanovený systém vyřazování entit, který vymezuje dobu jejich ukládání (skartační lhůta) a určuje typ skartační operace (trvalé uložení, předložení k přezkumu, automatické zničení, zničení po jeho schválení uděleném správcem nebo export do archivu). Při posouzení se v rámci odborné prohlídky vyhodnocují a) metadata, b) obsah dokumentu nebo c) metadata a obsah dokumentu. V případě, že skartační režim uplatňuje určený původce zřizující správní archiv podle § 69 odst. 1 zákona č. 499/2004 Sb., nepovažuje se podle § 69 odst. 4 zákona předání dokumentů ze spisovny do správního archivu za skartační operaci a lhůta stanovená pro uložení dokumentů ve spisovně ve spisových řádech není skartační lhůtou; pro převod dokumentu mezi spisovnami (například po odtajnění spisu) platí část věty před středníkem obdobně.
Skartační znak	§ 2 písm. r) zákona č. 499/2004 Sb.: Označení dokumentu, podle něhož se dokument posuzuje ve skartačním řízení.
Spisový a skartační plán	§ 66 odst. 2 zákona č. 499/2004 Sb.: Spisový a skartační plán obsahuje seznam typů dokumentů roztříděných do věcných skupin s vyznačenými spisovými znaky, skartačními znaky a skartačními lhůtami.
Spolehlivost	Věrohodnost, solidnost.
Stejnopis	§ 16 odst. 3 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby: Stejnopisem je jedno ze shodných násobných vyhotovení dokumentu nesoucí s tímto dokumentem shodné autentizační prvky; za shodné násobné vyhotovení dokumentu v analogové podobě se považuje rovněž doslovně shodné vyhotovení dokumentu v digitální podobě a naopak, pokud autentizační prostředky k nim připojila tatáž osoba; za stejnopis se považuje rovněž druhopis, pokud tak stanoví jiný právní předpis.

5 VMV čá. 64/2012 (část II), národní standard pro elektronické systémy spisové služby.

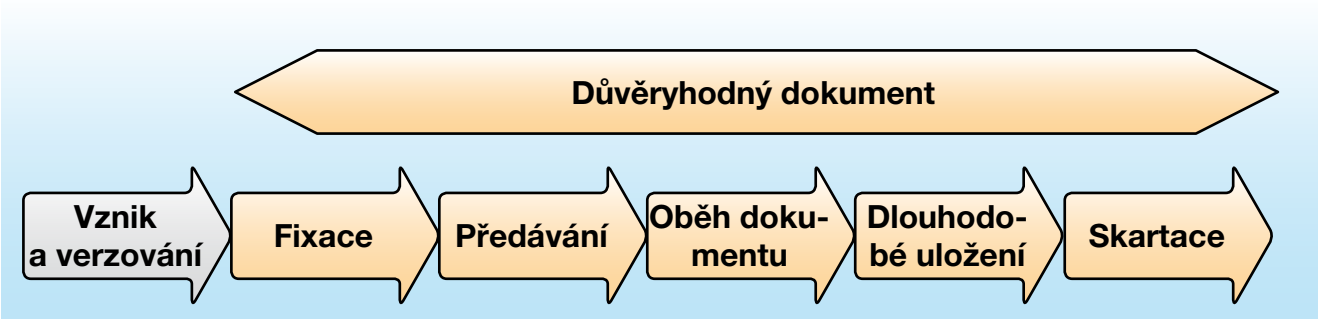
TERMINOLOGIE

Termín	Význam
Určený původce	Původce, který má dle zákona povinnost vést spisovou službu tak, jak stanoví § 63 zákona č. 499/2004 Sb., v platném znění.
Uznávaná elektronická značka	Uznávanou elektronickou značkou se rozumí elektronická značka založená na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.
Uznávaný elektronický podpis	Uznávaným elektronickým podpisem se rozumí: a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby, b) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie.
Validace	Ověření integrity dokumentu, kompletnosti metadat a stavu bezpečnostních prvků.
Věrohodnost	Hodnověrnost, spolehlivost.
XAdES	XML Advanced Electronic Signatures je rozšířením standardu XML-DSig, který slouží k podepisování XML dokumentů. Definován ETSI TS 101 903.
XML	eXtensible Markup Language – obecný značkovací jazyk.
Vyřazování dokumentů	Jedná se o proces, v jehož průběhu se posuzují dokumenty určené k vyřazení a na jehož konci je dokument předán do nadřízeného archivu, skartován nebo mu je posunuta skartační lhůta.
Zaručený elektronický podpis	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.

3 ÚVOD

Cílem tohoto dokumentu je vytvořit definici právně nezpochybnitelného dokumentu v elektronické podobě, který by byl akceptovatelný jak pro státní správu a samosprávu, tak i pro komerční a soukromou sféru.

Autoři si kladli za cíl definovat „důvěryhodný dokument“ v rámci jeho životního cyklu, tedy od jeho zafixování do nezměnitelné podoby až po jeho archivaci nebo zničení. Týká se tedy oblastí předávání dokumentu, oběhu dokumentu uvnitř organizace, ukládání dokumentu zaručující jeho nezměnitelnost a nakonec procesů jeho skartace a následné likvidace. Dokument se nezabývá oblastmi, jako jsou vznik a schvalování nezafixovaného dokumentu, jeho verzování a konverze dokumentů.



Obrázek 1: Osa životního cyklu dokumentu

Příkladem nezpochybnitelného „důvěryhodného“ dokumentu v historii může být založení Univerzity Karlovy[6]. Pražská univerzita byla založena nejméně třemi akty, totiž zakládající listinou papeže (bulou) Klementa VI., potvrzenou v Avignonu 26. ledna 1347, nadační listinou Karla IV. ze dne 7. dubna 1348 (udělení imunity univerzitě Karlem IV. před zásahy světské moci) a konečně tzv. Eisenašským diplomem ze 14. ledna 1349 (potvrdil Karel IV. jako římsko-německý král).

Je tedy známo, kdo založil univerzitu (**původ dokumentu**). Akt byl zafixován bulou, dokumentem s pečetí a následně diplomem (čímž byla zaručena **neměnnost a neporušitelnost**). Kromě toho je možné jednoznačně identifikovat **původce dokumentů – autority** dané doby (v čase) jako např. Klement VI. a Karel IV. A nakonec čitelnost byla zabezpečena péčí o tak důležitý dokument (archivy, knihovna, trezor apod.).

Podobně musí být důvěryhodnost zabezpečena i dnes u elektronických dokumentů. Kromě technických a technologických nástrojů je však nutné pracovat také s organizačními a bezpečnostními opatřeními v oblasti správy dokumentů dané organizace. Nelze totiž od sebe oddělovat důvěryhodnost dokumentu samotného od způsobu, jak s ním zacházíme. Sebelépe ošetřený dokument sám o sobě nemůže být důvěryhodný, pokud není ošetřeno i okolí tohoto dokumentu.

6 http://cs.wikipedia.org/wiki/Univerzita_Karlova

4 DŮVĚRYHODNÝ DOKUMENT

Východiska a zdůvodnění

Definice důvěryhodného dokumentu (v elektronické formě) vychází z přirozených požadavků, které jsou tradičně kladeny i na klasické listinné dokumenty. Základním požadavkem je **pravost dokumentu**, tedy skutečnost, že dokument je **originální, nefalšovaný, nezměněný a úplný**. Protože práce s originálními (původními) listinami není vždy praktická, často se používají kopie, jejichž shoda s originálem je ověřena vidimací (viz zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů /zákon o ověřování/, v platném znění). Zatímco v listinné podobě existuje zpravidla jediný originál (s výjimkou např. stejnopisů), v elektronické podobě je originál a jeho digitální kopie nerozeznatelná – to se samozřejmě týká i elektronicky podepsaného dokumentu. Proto je nutné všechny identické kopie elektronického dokumentu považovat za rovnocenné s původním dokumentem.

Písemnosti jsou **obvykle opatřeny podpisem**, například autora, jednající osoby nebo osoby zodpovídající za správnost. Pokud písemnost zakládá právní jednání, vždy se vyžaduje podpis jednajícího (viz § 561 odst. 1 zákona č. 89/2012 Sb., občanský zákoník).

Náš právní řád taxativně nevymezuje, co se rozumí (vlastnoručním) podpisem ani jaké jsou jeho funkce. V praxi se využívají 3 základní funkce podpisu:

1. označovací – identifikace podepisující osoby, toho, kdo učinil právní úkon,
2. deklarační – potvrzení projevu vůle,
3. důkazní – ověření totožnosti jednajícího.

Vycházejíce z těchto funkcí podpisu je zřejmé, že důvěryhodný dokument (v listinné i elektronické podobě) **musí být podepsaný**. Aby bylo možné podepsaný dokument považovat za důvěryhodný, musí být zřejmé, za jakým účelem byl dokument podepsán. Účel může plynout z typu podepsaného dokumentu (například smlouva je podepsána za účelem vyjádření vůle podepisujících stran splnit povinnosti stanovené ve smlouvě) nebo z explicitního prohlášení účelu podpisu, které je buď součástí podepsané zprávy, připojené doložky, nebo evidovaného externího dokumentu (podpisový řád).

V případě dokumentu v elektronické podobě je vyžadován elektronický podpis nebo elektronická značka. I zde je však nutné zkoumat, **za jakým účelem a kým byl tento elektronický podpis učiněn**. Pokud například dokument v elektronické formě vznikl digitalizací listinného dokumentu (konverzí z listinné formy do elektronické formy), elektronický podpis zpravidla neučinila tatáž osoba, která podepsala listinný dokument, ani účel elektronického podpisu nebyl shodný s účelem vlastnoručního podpisu listinného dokumentu. V případě digitalizovaného dokumentu je účelem elektronického podpisu nebo značky prokázání, že digitální kopie je vizuálně shodná s digitalizovanou písemností a čitelná (odpovídá tzv. vidimaci). Analogické závěry lze učinit v případě konverze formátu dokumentu v elektronické podobě.

Důvěryhodný dokument může být **podepsaný originální (původní) dokument**, jeho **kopie** (ověřená v případě listiny) nebo **replika** (identická kopie v případě dokumentu v elektronické podobě), případně konverze, v každém případě musí být ověřitelný **původ dokumentu**, tedy musí být ověřitelný původce originálního dokumentu[7].

Z definice uznávaného elektronického podpisu (viz § 11 odst. 3 zákona 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů /zákon o elektronickém podpisu/, ve znění pozdějších předpisů) vyplývají jeho základní vlastnosti. Uznávaný elektronický podpis je:

a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby,

b) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie.

Uznávaný podpis musí samozřejmě splňovat všechny požadavky kladené na zaručený elektronický podpis:

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.

Ke splnění základních funkcí podpisu je třeba pro důvěryhodný dokument v elektronické podobě v oblasti orgánů veřejné moci vyžadovat uznávaný elektronický podpis, v soukromé sféře vyžadovat zaručený elektronický podpis a doporučit uznávaný elektronický podpis. Tento požadavek ale nestačí splnit pouze k okamžiku vytvoření podpisu, výše uvedené 4 vlastnosti zaručeného elektronického podpisu je nutné zaručit v dlouhodobém časovém horizontu. Vzhledem k omezené časové platnosti certifikátů, které jsou vydávány k ověření platnosti uznávaných elektronických podpisů, a dále vzhledem k – v průběhu času – obecně klesající bezpečnosti kryptografických algoritmů použitých k vytvoření zaručených elektronických podpisů je nutné požadované vlastnosti fixovat prostřednictvím periodicky aplikovaných **časových razítek**, ve shodě s uznávanými technickými standardy. Tato fixace dokumentu je poměrně náročná služba, kterou by měl zajišťovat kvalifikovaný poskytovatel služeb dlouhodobého úložiště dokumentů v elektronické podobě.

Dalším požadavkem je **čitelnost dokumentu**. Čitelnost znamená, že lze přímo nebo s použitím technických prostředků **získat datový obsah dokumentu**. Je vhodné poznamenat, že požadavek na čitelnost dokumentu neznamená nutně, že je vždy možné získat informaci obsaženou v dokumentu (například v případě šifrovaných dokumentů je nutné navíc znát příslušné kryptografické algoritmy, jejich parametry a klíče).

7 Dle § 4 vyhlášky č. 259/2012 Sb. je nutné uchovávat nejméně po dobu 3 let předlohu dokumentu, který byl převeden.

Je nutné poznamenat, že podstatně složitější je situace v případě dlouhodobé čitelnosti formátů elektronických dat, které obsahují multimediální obsah, jako je zvuk a video, proto si tento dokument neklade za cíl pokrýt tuto oblast.

Definice

Digitální dokument[8] je důvěryhodný, pokud jsou splněny následující požadavky:

- Jedná se o originální (autentický, původní) dokument nebo jeho odvození z originálního dokumentu (např. stejnopis či jeho konvertovanou verzi).
- Lze jednoznačně určit původ dokumentu.
- Lze jednoznačně ověřit, že nedošlo k porušení integrity dokumentu[9].
- V případě kopie, repliky nebo konverze lze doložit shodu s originálem.
- Je zaručena jeho čitelnost.
- Lze jednoznačně prokázat existenci dokumentu v čase.

Digitální dokument ztrácí svou důvěryhodnost zejména tehdy:

- je-li nečitelný;
- došlo-li k porušení jeho integrity;
- není-li možno jednoznačně prokázat platnost bezpečnostních prvků zaručujících jeho důvěryhodnost (elektronický podpis, časové razítko, hashovací algoritmus) v době jeho vzniku.

8 Důvěryhodný dokument je právně nezpochybnitelný. Neměnnost a neporušitelnost dokumentu lze obtížně zaručit, pouze lze činit opatření, která to znesnadňují. Místo toho lze požadovat jednoznačnou detekovatelnost porušení integrity dokumentu.

9 Definice důvěryhodného dokumentu obsahuje požadavek na porušitelnost integrity dokumentu, který zahrnuje i případnou změnu dokumentu dynamickými prvky.

5 SLUŽBY PRO VZNIK A ZACHOVÁNÍ DŮVĚRYHODNOSTI DOKUMENTU

Z důvodu zaručení důvěryhodnosti dokumentu z dlouhodobého hlediska je nutné využívat komplex služeb důvěryhodných poskytovatelů, jako např.:

- ověřování elektronického podpisu/značky;
- ověřování certifikátů, na nichž je založen elektronický podpis/značka, časové razítko;
- registr elektronických identit osob (v ČR dnes neexistuje);
- zachovávání/udržování síly kryptografického mechanismu elektronického podpisu/značky a časového razítka;
- služba fixace dokumentu formou elektronické značky a/nebo časového razítka;
- služba převodu do standardizovaného archivního formátu;
- služba autorizované konverze, která by umožnila konvertovat i další formáty kromě PDF/A – minimálně AdES formáty.

Tyto služby mohou být součástí dlouhodobého úložiště, není to však bezpodmínečně nutné.

Pro zajištění dlouhodobé důvěryhodnosti dokumentu je vhodné kombinovat při ukládání vhodný formát elektronicky podepsaného dokumentu[10] a služby dlouhodobého elektronického úložiště – automatické označování elektronickými značkami a časovými razítky, automatická kontrola elektronických podpisů a jejich kvalifikovaných certifikátů, archivace logů, zajištěné uživatelské přístupy a vhodný zálohovací mechanismus.

10 PDF/A-1 – ISO 19005-1:2005, PDF/A-2 – ISO 19005-2:2011, PDF/A-3 – ISO 19005-3:2012. Rozhodnutí Evropské komise ze dne 25. února 2011 č. K(2011) 1081, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných (definující vhodné formáty dat), normy ETSI TR 102 923 V1.1.1 (2010-07) PDF Advanced Electronic Signatures (PAdES), ETSI TS 101 903 V1.4.2 (2010-12) XML Advanced Electronic Signatures (XAdES), ETSI TS 101 733 V2.1.1 (2012-03) CMS Advanced Electronic Signatures (CAdES).

6 DŮKAZNÍ MATERIÁL

Důkazní materiál o důvěryhodnosti dokumentu by měl dokazovat, že daný dokument splňuje po celou dobu svého životního cyklu (od chvíle jeho zafixování a následně po dobu jeho uložení v důvěryhodném úložišti až k požadovanému datu) všechny požadavky kladené na „důvěryhodný dokument“.

„Důkazní materiál důvěryhodného dokumentu“ by měl obsahovat tyto komponenty:

- dokument samotný;
- základní metadata (sadu základních povinných metadat, která by měla být vždy součástí důkazního materiálu);
- záznam všech operací, kterým byl dokument podroben (např. konverze, tisk, export);
- informace o provedené konverzi (konverzní doložka), byla-li provedena;
- elektronický podpis podepisující osoby / el. značka označující organizace či osoby;
- elektronická značka úložiště a časové razítko dokumentující čas příjmu do úložiště;
- všechny bezpečnostní prvky (otisky) dokumentu a archivního balíčku;
- důkazní informace o ověření uznávaného elektronického podpisu / elektronické značky a kvalifikovaných certifikátů (crl, OCSP…);
- prohlášení o způsobu vkládání, ověřování a uchovávání dokumentů v důvěryhodném úložišti s odkazem na vnitřní politiku organizace / certifikovaný systém;
- elektronická značka a časové razítko vztahující se k důkaznímu materiálu definující čas generování důkazního materiálu.

Formát důkazního materiálu bude definován v připravovaném dokumentu „Důvěryhodný dokument – důkazní materiál a jeho formát“.

7 ANALÝZA ZPŮSOBŮ ZTRÁTY DŮVĚRYHODNOSTI

Tato kapitola diskutuje možné situace, jejichž následkem dochází ke ztrátě důvěryhodnosti dokumentu. Předmětem analýzy jsou dokumenty v digitální podobě. V tomto kontextu lze operovat s pojmem „replika“ ve významu dokonalé „kopie“, kterou nelze fyzikálně odlišit od originálu; naopak se analýza nezabývá dokumenty analogového charakteru s jejich odlišující charakteristikou – šumem, který existenci replik prakticky znemožňuje.

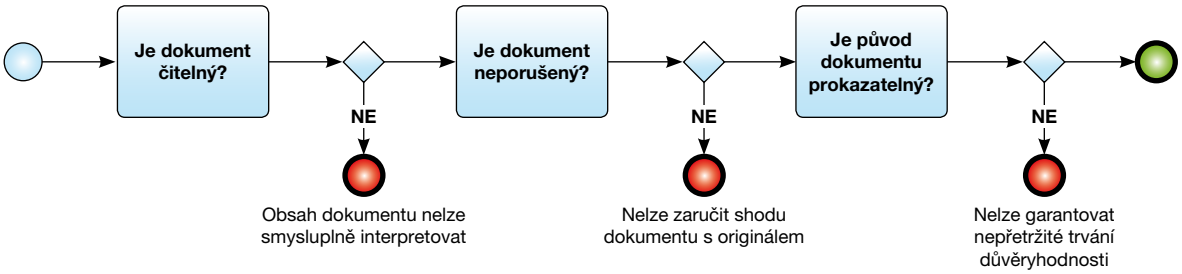
Cílem rozboru různých forem selhání důvěryhodnosti je pomoc při pochopení, na jakých principech je konstrukt „důvěryhodnosti“ či „pravosti“ vystavěn, pomocí jakých prostředků jsou tyto principy prosazovány, jaká jsou jejich inherentní omezení a jak lze tato omezení překonat.

Analýza vychází z předpokladu, že ověření důvěryhodnosti je prováděno určitým mechanismem, který na základě vstupů (ověřovaný dokument a jeho metadata, data reprezentující originální dokument, případně další údaje) rozhoduje, zda lze ověřovaný dokument považovat za pravý.

Ztráta důvěryhodnosti může nabývat dvou obecných podob:

- Nepravý dokument je ověřovacím mechanismem *nesprávně označen jako pravý*. Takový typ selhání bude v dalším textu označováno jako typ I.
- Pravý dokument je ověřovacím mechanismem *nesprávně označen jako nepravý*. Tento druh selhání bude v dalším textu označován jako typ II.

Důvěryhodný dokument musí podle své definice splňovat několik kritérií. Pokud je alespoň jedno kritérium narušeno, dochází ke ztrátě důvěryhodnosti, jak ilustruje diagram níže. Přehled těchto kritérií a jim vlastních režimů selhání je rozveden v následujících sekcích.

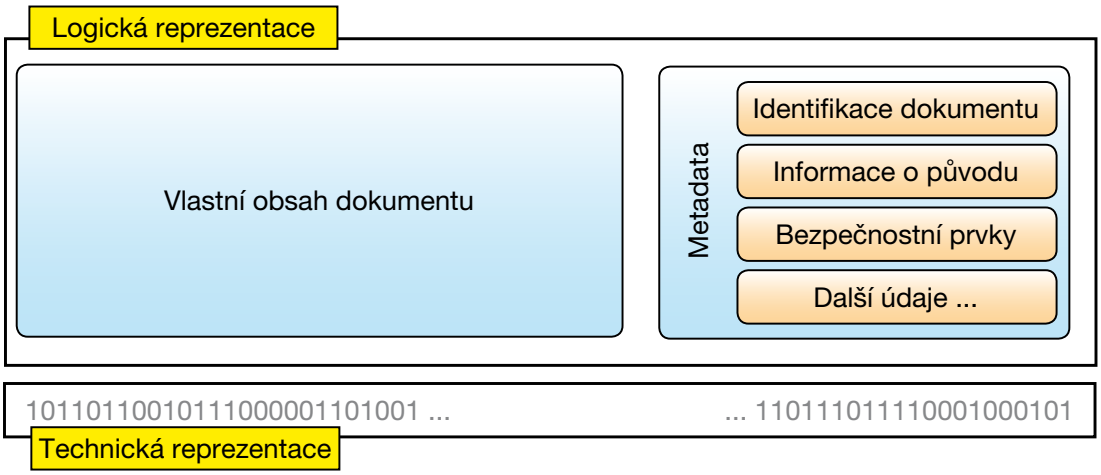


Obrázek 2: Způsob vyhodnocení důvěryhodnosti dokumentu

Čitelnost dokumentu

Aby bylo možné s dokumentem jakkoliv nakládat, je nutné zajistit, aby byl uživatel schopen získat informace, které jsou pro něj srozumitelné a zároveň přesně reprezentují obsah dokumentu. Možná selhání mohou nabývat dvou podob: technické a sémantické. Tyto režimy vyplývají ze způsobu, jakým jsou elektronické dokumenty ukládány a zpracovávány; vztah technické (fyzické) a logické (sémantické, informační) podoby dokumentu, včetně typické struktury logické reprezentace, ilustruje obr. č. 3.

Selhání technického charakteru znamená, že dokument, resp. dokument reprezentující bitovou posloupnost, nelze extrahovat ze samotného nosiče. Protože extrakce dokumentu není přímou podmínkou důvěryhodnosti (jedná se o prerekvizitu dalších kritérií, zejména podmínky integrity), nejsou u tohoto aspektu rozlišována selhání typu I a II. Obranou proti selhání je zejména eliminace kritické závislosti na nosiči informací – typickým přístupem je zavedení vhodné formy redundance, např. využitím několika nosičů současně, reprezentace obsahu dokumentů odolná vůči náhodným chybám (Reed-Mullerovo kódování) apod.



Obrázek 3: Vztah technické a logické podoby dokumentu

Podstatou ***selhání sémantického charakteru*** je situace, kdy obsah dokumentu nelze správně interpretovat. V případě elektronických dokumentů, které ve své přirozené podobě nejsou přímo čitelné lidskými smysly, má toto selhání zásadní vliv. Přirozenou podobou rozumíme statickou posloupnost bitů; pro jejich další interpretaci se využívá technických instrukcí v podobě specifikací datových protokolů a formátů, které jsou implementovány jako tzv. dekodér.

- Selhání typu I znamená, že nesprávně zformovanou posloupnost bitů převádí dekodér do podoby validního dokumentu. Lze se domnívat, že taková situace nastává spontánně jen zřídka (jako důsledek chyb ve specifikaci formátu). Častěji se lze setkat s případem záměrného chování, kdy se dekodér snaží uživateli poskytnout podvržené informace. Je nutné si uvědomit, že předmětem dekódování nebývá jen samotný obsah dokumentu, ale i jeho související metadata. Selhání na této úrovni může být tudíž obtížně detekovatelné. Typickým způsobem obrany je využití referenčních dokumentů, u nichž je přesně definována podoba očekávaného dekódovaného výstupu.
- Selhání typu II v tomto kontextu znamená, že správně zformovanou posloupnost bitů nebyl schopen dekodér korektně zpracovat. Taková situace může nastat např. v důsledku postupného vývoje datového formátu a souvisejícího opouštění podpory starších verzí nebo jako následek rozporů ve specifikaci. Vhodným protiopatřením je využívání takových datových formátů, které jsou standardizované, otevřené a verzovatelné, pokud možno též i prověřené praktickým použitím, a tudíž obsahující minimum chyb či víceznačností.

Integrita dokumentu

Podstatou aspektu integrity je požadavek, aby bylo možné ověřit, zda se informace obsažené v dokumentu přesně shodují s obsahem originálního dokumentu. Přestože je teoreticky vhodnější takové porovnání provádět na sémantické úrovni (kontroluje se identita informací), často se z praktických důvodů provádí na úrovni technické reprezentace (porovnává se shodnost posloupnosti bitů).

Dalším faktorem pro úvahy o ověřování integrity je skutečnost, že v případě přenosu informace v digitální podobě nedochází k „přenosu“ originálu ve fyzikálním smyslu. Digitální přenos spočívá v postupném vzniku mnoha (dočasných) replik původního dokumentu (takto lze popsat nejen přenos dokumentu v počítačových sítích mezi jednotlivými počítači, ale i přenos mezi vnitřními komponentami, mezi úložištěm a operační pamětí atd.). Tento faktor má zásadní význam: ověřování integrity elektronického dokumentu probíhá v naprosté většině případů za nepřítomnosti originálu a je tudíž nutné spolehnout se na nepřímé metody.

Přímá metoda ověření integrity porovnáním úplného obsahu kontrolovaného dokumentu s korespondujícím originálním dokumentem je triviální a neposkytuje prostor pro selhání. Jak však bylo uvedeno výše, tato metoda může být nejen nepraktická, ale v prostředí ryze elektronických komunikací také vyloučená.

Soudobé ***nepřímé metody pro ověření integrity*** vycházejí z konceptu otisku dokumentu. Otiskem (hashem) se rozumí informace odvozená z obsahu dokumentu, jejíž informační kapacita je ve srovnání se zdrojovým dokumentem řádově menší (často má z praktických důvodů pevně danou délku bitové posloupnosti), a tudíž postrádá vlastnost injektivity mezi množinou všech možných dokumentů a množinou všech možných otisků. Otisk je obvykle uložen jako součást metadat v rámci dokumentu, ale může být přenášen i nezávisle.

Nepřímé metody ověření integrity založené na otiscích se vyznačují následujícími režimy selhání:

- Selhání typu I znamená, že pro otisk H_A, který byl odvozen z dokumentu A, lze najít odlišný dokument B, jehož otisk H_B je identický s otiskem H_A. Tato situace se nazývá kolizí a teoreticky nastává nevyhnutelně u všech algoritmů, které produkují otisky pevné délky. Protiopatřením je volba takových algoritmů, u nichž je cílené vyhledávání kolizních dokumentů výpočetně extrémně náročné. Současně je nutné brát do úvahy, že v průběhu času je síla hashovacího algoritmu klesající (úměrně ke zvyšování dostupného výpočetního výkonu, v případě průlomů v oblasti kryptoanalýzy se může měnit skokově), proto by mechanismus pro ověřování integrity měl být schopen využívat rozšiřitelnou sadu hashovacích algoritmů[11].
- Selhání typu II by nastalo, pokud by pro konkrétní dokument existovalo více různých otisků. V případě deterministických algoritmů odvozování otisků tato situace nemůže nastat; nedeterministické metody ze své podstaty postrádají v tomto kontextu smysl. Selhání typu II však může nastat v případech, kdy lze tentýž dokument reprezentovat několika různými způsoby. Protiopatřením je volba takových datových formátů, které výslovně specifikují jednoznačnou kanonickou reprezentaci dokumentu, která je následně využívána pro tvorbu otisků.

11 Kromě univerzálních hashovacích funkcí (kam patří zejména rodiny algoritmů MD, SHA, bezpečnostně slabé kontrolní součty z rodiny CRC apod.) lze pro ověřování integrity využít i alternativních prostředků, zejména tzv. kódů pro autentizaci zpráv (Message Authentication Code, MAC). Ty se od prostých hashovacích funkcí liší tím, že pro tvorbu otisku využívají nejen obsah dokumentu, ale i doplňkovou informaci (šifrovací klíč) sdílenou pouze mezi stranami, které dokumentem disponují. Právě přítomnost sdíleného klíče, resp. obtíže s jeho bezpečnou distribucí mezi komunikujícími stranami jsou však důvodem, proč se autentizační kódy MAC využívají pro zabezpečení integrity dokumentů jen zřídka.

ANALÝZA ZPŮSOBŮ ZTRÁTY DŮVĚRYHODNOSTI

Při diskusi režimů selhání integrity je nutné připomenout, že ke ztrátě integrity může dojít nejen změnou vlastního obsahu dokumentu, ale též modifikací otisku hrajícího roli reprezentanta obsahu originálního dokumentu nebo obdobných metadat. Z praktických důvodů je většina elektronických dokumentů konstruována tak, že obsah spolu s metadaty tvoří jeden fyzický soubor. Je proto nutné zohlednit, jakým způsobem je zajištěna jeho integrita jak jednotlivých částí, tak i výsledného celku. Lze konstatovat, že hlavním úkolem soudobých metod pro ověření integrity je ochrana proti spontánním změnám obsahu; obecně jsou tyto metody jen málo rezistentní vůči cílenému útoku (není to ostatně ani jejich rolí).

Původ dokumentu

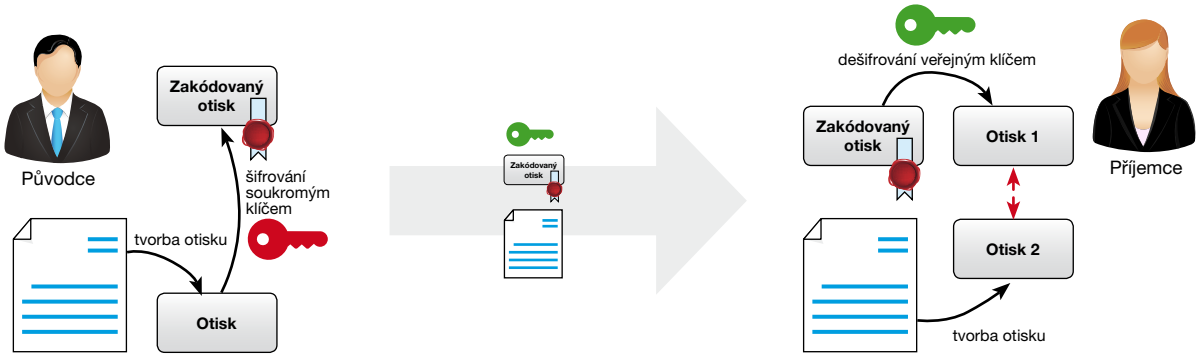
Souhrnné označení „informace o původu dokumentu“ zahrnuje řadu dílčích aspektů. Patří mezi ně:

- identifikace původce dokumentu,
- datum a čas vzniku dokumentu,
- chronologie všech manipulací s potvrzením, že důvěryhodnost byla zachována.

Narušením libovolného aspektu v časové kontinuitě existence dokumentu dochází k celkové ztrátě důvěryhodnosti.

Identita původce

Soudobé metody pro důvěryhodnou identifikaci původce dokumentu jsou založeny na technologiích elektronického podpisu, realizovaných prostředky asymetrické kryptografie. Podpis má obvykle podobu zakódovaného otisku dokumentu, který byl vytvořen zašifrováním běžného otisku pomocí soukromého šifrovacího klíče. Z podpisu lze pomocí příslušného veřejného klíče extrahovat původní otisk, který lze porovnat s ověřovaným dokumentem. Postup ilustruje následující schéma.



Obrázek 4: Vytvoření a ověření elektronického podpisu

Vychází se z předpokladu, že pouze zakódovaný otisk je schopen vytvořit výhradně držitel soukromého klíče. Každý příjemce, který disponuje souvisejícím veřejným klíčem, je schopen vazbu podpis–dokument ověřit. Aby však bylo možné hovořit o „podpisu“, je nezbytné, aby byla ustavena důvěryhodná vazba mezi veřejným klíčem a identitou držitele soukromého klíče. Tuto vazbu poskytuje infrastruktura PKI (Public Key Infrastructure) a její klíčová součást – certifikační autorita (CA), tedy třetí strana, jejíž důvěryhodnost je uznávaná jak původcem, tak příjemcem. Ověření původce je tedy postavené na předpokladu, že podpis vytvořil výhradní držitel určitého soukromého klíče, jehož identitu garantuje certifikační autorita (tato garance má formu tzv. certifikátu).

Možné režimy selhání jsou následující:

- Selhání typu I/a, kdy podpis podvrženého dokumentu byl vyhodnocen jako pravý, přičemž tento podpis byl vytvořen soukromým klíčem deklarovaného původce. Taková situace nastává nejčastěji v důsledku získání neautorizovaného přístupu k soukromému klíči. Toto riziko lze eliminovat mechanickými prostředky jen částečně, jsou vyžadovány explicitní kroky ze strany držitele. Typicky se jedná o uložení klíče v bezpečném výpočetním prostředí (např. v hardwarových modulech HSM). Dalším obvyklým protiopatřením je omezení časové platnosti certifikátů a pravidelná kontrola seznamů revokovaných certifikátů, které CA publikují.
- Selhání typu I/b nastává tehdy, pokud útočník byl schopen odvodit soukromý klíč, aniž by k němu měl přímý přístup; získává tak možnost vystupovat pod identitou skutečného držitele. Většina používaných algoritmů asymetrické kryptografie se vyznačuje skutečností, že veřejný klíč obsahuje skryté matematické struktury, které lze využít k odvození příslušného tajného klíče. Bezpečnost se odvozuje od extrémní výpočetní náročnosti takového postupu, avšak pravděpodobnost kompromitace není nulová a v průběhu času roste. Zejména dopad, který bude na tuto oblast mít intenzivnější rozvoj kvantových výpočetních systémů, lze v současnosti odhadovat jen obtížně, proto návrh potenciálních protiopatření je komplikovaný. Obecně však lze doporučit, aby datový formát pro uložení dokumentu umožňoval uložit různé druhy elektronických podpisů.
- Selhání typu I/c by mohlo nastat tehdy, pokud by jedna datová struktura využívaná pro tvorbu elektronického podpisu (zejména její část obsahující otisk) odpovídala více různým dokumentům. Výsledný elektronický podpis by pak byl platný pro všechny dokumenty s tímto (kolizním) otiskem. Protiopatření se skládají, obdobně jako v části Integrita dokumentu, z využívání dostatečně bezpečných metod pro tvorbu otisků. Je též vhodné, aby součástí podepisované datové struktury byl i unikátní, na obsahu dokumentu nezávislý prvek, např. sériové číslo.
- Selhání typu I/d, kdy podpis podvrženého dokumentu je vyhodnocen jako pravý, přičemž tento podpis nebyl vytvořen soukromým klíčem deklarovaného původce. Z toho vyplývá, že i veřejný klíč (resp. certifikát) využívaný příjemcem dokumentu je nevyhnutelně odlišný, avšak daná certifikační autorita jej nesprávně spojuje s identitou deklarovaného původce. Toto selhání lze definovat jako ztrátu důvěryhodnosti certifikační autority. Vhodným protiopatřením je využívání služeb jen takových CA, u nichž je riziko vzniku takového stavu minimalizováno např. akreditací.
- Selhání typu II nastává, pokud se přeruší vazba mezi dokumentem a podpisem navzdory tomu, že v nějakém časovém momentu byla tato vazba nezpochybnitelně platná. Příčin může být několik, avšak typicky k tomuto selhání dochází v důsledku exspirace příslušného certifikátu, a tudíž ukončení garancí, které certifikační autorita k tomuto certifikátu poskytovala. Jedná se tedy o změnu na úrovni abstraktního kontraktu – po technické stránce nedochází k žádné změně, mechanické ověření vazby mezi podpisem a dokumentem je nadále úspěšné. Možná protiopatření proti této formě selhání proto musí být realizována taktéž na úrovni kontraktu. Příkladem může být konvence, že kontinuitu důvěryhodnosti certifikátu a jím realizovaných elektronických podpisů lze prodloužit i nad rámec doby jeho původní časové platnosti souborem vhodných opatření pro tzv. Long Term Validation (LTV). Návrh takových opatření je obsažen např. v normách institutu ETSI, které se zabývají elektronickým podpisem (PAdES, XAdES, CAdES).

Čas vzniku dokumentu

Klíčovým nástrojem pro důvěryhodné svázání dokumentu s nějakým časovým momentem je tzv. časové razítko. Je vystavováno certifikační autoritou a garantuje, že daný dokument (v podobě reprezentované otiskem) existoval před vystavením časového razítka.

Konceptuálně lze na časové razítko pohlížet jako na specifický dokument, jehož původcem je autorita pro vydávání časových razítek (Timestamping Authority, TSA) a jehož obsah se (zejména v prostředí infrastruktury PKI) skládá z následujících klíčových částí:

- otisk dokumentu převzatý ze žádosti o vystavení časového razítka (TSA neověřuje jeho správnost, neboť obvykle nemá k dispozici zdrojový dokument),
- sériové číslo časového razítka v prostředí TSA,
- vlastní časový údaj (včetně informace o jeho přesnosti).

Metodiky pro konstrukci časových razítek (např. RFC 3161) doporučují, aby identita žadatele o časové razítko *nebyla součástí* jeho obsahu. Výsledný „dokument" je poté opatřen elektronickou značkou TSA (tj. automaticky produkovaným elektronickým podpisem). Časové razítko tedy poskytuje pouze informaci o tom, že daný otisk dokumentu existoval před určitým časovým okamžikem.

Diskusi o možných selháních důvěryhodnosti časových razítek lze na základě uvedených principů převést na otázku důvěryhodnosti (zejména aspektů čitelnosti, integrity a identity TSA jako původce) tohoto typu dokumentů. Významným faktorem pro důvěryhodnost je vazba časového razítka na certifikát TSA (v infrastruktuře PKI) – z toho vyplývá, že samotné časové razítko má omezenou dobu platnosti v intervalu od data vystavení po datum exspirace použitého certifikátu. Věrohodnost samotného časového údaje je pak dána abstraktním kontraktem, typicky tzv. politikou pro vydávání časových razítek, kterou TSA publikuje.

Chronologie manipulací s dokumentem

Přesný název tohoto aspektu důvěryhodnosti by měl znít „chronologie manipulací s metadaty dokumentu", neboť vlastní obsah zafixovaného dokumentu měnit nelze (z pohledu důvěryhodnosti dochází k porušení integrity).

Protože metadata tvoří klíčové prostředky pro udržování a ověřování důvěryhodnosti dokumentu, je nutné zajistit, aby nedošlo k jejich narušení po celou dobu existence dokumentu. Obecně lze nakládání s metadaty rozdělit na úkony povolené (věrohodnost dokumentu nesnižující, např. přidání nového časového razítka nebo změna metadat, která nemají vliv na důvěryhodnost) a zakázané (kompromitující věrohodnost, např. záměna elektronického podpisu, odstranění informace o neúspěšném ověření důvěryhodnosti).

- Selhání typu I znamená, že došlo k nedetekované zakázané manipulaci. Příkladem vhodného protiopatření je využití techniky řetězení, kdy jedinou povolenou manipulací je inkrementální přidávání atomických bloků metadat, přičemž každý přidávaný blok obsahuje důvěryhodnou vazbu na přímo předcházející blok a jeho obsah. Případné změny obsahu stávajících bloků nebo jejich odstranění pak nevyhnutelně naruší existující řetězec vazeb.
- Selhání typu II/a vzniká tehdy, kdy povolená manipulace má za následek ztrátu důvěryhodnosti. Využitím vhodně navržených formátů pro reprezentaci dokumentů a jejich metadat lze toto riziko eliminovat.

- Selhání typu II/b vzniká v důsledku absence povolené (resp. v dané situaci vyžadované) manipulace. Tento typ selhání vyplývá ze skutečnosti, že většina artefaktů reprezentujících původ dokumentu má omezenou časovou platnost. Pokud není platnost nějakou formou prodloužena, pak striktně vzato nenávratně zaniká, není-li možné důvěryhodnost dokumentu ověřit jinými prostředky. Protiopatření spočívají ve využití postupů Long Term Validation, které je nutné aplikovat po celou dobu existence dokumentu.

8 NAVAZUJÍCÍ AKTIVITY PRACOVNÍ SKUPINY ICTU – ARCHIVNICTVÍ

Pracovní tým Správa a ukládání důvěryhodných dokumentů

Pracovní tým „Správa a ukládání důvěryhodných dokumentů“ se zabývá elektronickými dokumenty v jejich celém životním cyklu. Od jejich vzniku, evidence, konverze do vhodného formátu, ukládání v úložišti a následného procesního zpracování až po jejich skartaci či předání do státního archivu. Těmito činnostmi se musí prolínat jasná nit vzájemně na sebe navazujících postupů a technologií, které mají za cíl uchovat po celou dobu „života“ jejich důvěryhodnost.

Jak bylo zmíněno v kapitole **Důvěryhodný dokument**, pro zajištění dlouhodobé důvěryhodnosti dokumentu je vhodné kombinovat při ukládání vhodný formát elektronicky podepsaného dokumentu a služby dlouhodobého elektronického úložiště.

Proto se pracovní tým postupně zabývá všemi souvisejícími postupy a technologiemi:

- službou fixace dokumentu formou elektronické značky/podpisu a/nebo časového razítka;
- službou převodu do standardizovaného archivního formátu;
- službou autorizované konverze, která by umožnila konvertovat i další formáty kromě PDF/A – minimálně AdES formáty;
- ověřováním elektronické značky/podpisu;
- ověřováním certifikátů, na nichž je založen elektronický podpis/značka, časové razítko;
- problematikou elektronické identity osob a jejich mandátu k podpisu dokumentů (mandátní registr);
- zachováváním/udržováním síly kryptografického mechanismu elektronického podpisu/značky a časového razítka;
- potřebnými službami a technologiemi elektronického úložiště z pohledu dlouhodobého ukládání informací – řízení přístupů (uživatelů/systémů), vytváření a ošetření logů systému – zabezpečení tzv. auditní stopy, řešení automatizovaných činností počínaje označováním dokumentů elektronickými značkami, časovými razítky, jejich validací apod.;
- volbou vhodných zálohovacích mechanismů.

Výstupem analýzy zmiňovaných oblastí bude připravovaný dokument, který si klade za cíl sdružovat na jediném místě potřebné informace vztahující se ke správě a dlouhodobému ukládání dokumentů jak z pohledu kontextu legislativy České republiky, tak i EU.

Tento dokument by měl pomoci naplňovat i vizi „digitálního obchodního styku“.

Pracovní tým Důkazní materiál

Činnost pracovního týmu „Důkazní materiál“ navazuje na pracovní tým „Správa a ukládání důvěryhodných dokumentů“. Obě aktivity, i přes určité shodné znaky, představují velmi odlišné činnosti. V případě „důvěryhodných dokumentů“ se jedná fakticky o archivaci digitální podoby „papírových“ dokumentů, u „důkazního materiálu“ jde sice také o archivaci digitálních dat, ale značně fyzicky odlišných. V tomto případě jde o velmi širokou škálu důkazních materiálů (fotografie, audio, videomateriály, mailová korespondence, odposlechy atd.). V podstatě lze zjednodušeně říci, že se jedná o multimediální úložiště nejrůznějších druhů digitálních dat. Samozřejmě data tohoto typu se dotýkají široké škály institucí a jejich činností. Proto je v prvotní fázi nutné oslovit ke spolupráci značné množství expertů z institucí, kteří se s touto problematikou mohou setkat jako první a také k ní mají odborně co říci.

V první etapě je tedy potřeba oslovit řadu expertů, kteří pomohou s nastavením právního rámce „důkazního materiálu“.

Doposud byli osloveni experti z následujících organizací či orgánů:

- Nejvyšší státní zastupitelství (JUDr. Pavel Zeman, nejvyšší státní zástupce, osobně přislíbil spolupráci)
- Policejní prezidium ČR (v současné době v řešení)
- Notářská komora ČR (JUDr. Martin Foukal, prezident, osobně přislíbil spolupráci)
- právníci MV ČR a soukromé AK
- Právnická fakulta Masarykovy univerzity Brno (doc. JUDr. Radim Polčák, Ph.D., přislíbil neformální spolupráci)
- Soudcovská unie ČR (na doporučení doc. Polčáka osloven JUDr. Tomáš Lichovník, prezident Soudcovské unie ČR, v současné době v řešení)
- soudní znalci znaleckého ústavu Apogeo Esteem (vedoucí týmu je manažerem ICT divize znaleckého ústavu)

První schůzka je plánována v květnu 2014 a jejím cílem je potvrzení spolupráce oslovených expertů. Dále stanovení cíle, termínů a etapizace jednotlivých činností, řešení a určení rolí.

Předpokládáme, že v první etapě bude řešen právní rámec, ve druhé určení typů a formátů „důkazního materiálu“ a ve třetí pak technická realizace verifikace a ukládání.

Předpoklad dokončení všech tří etap je konec roku 2014.

9 ZÁVĚR

Hlavním cílem tohoto dokumentu bylo zavést definici důvěryhodného dokumentu a vyjmenovat služby, které jsou nezbytné pro efektivní zafixování, údržbu a používání důvěryhodných dokumentů. Narůstající množství dokumentů v elektronické podobě, které nejsou udržovány v důvěryhodném stavu, může v budoucnosti přinášet právní nejistotu a zapříčinit složité spory. V souvislosti s tím bylo upozorněno na přetrvávající nedostatky v zákonných úpravách, zejména v oblasti elektronické identifikace, elektronického identifikačního dokladu a fikce elektronického podpisu.

Lze očekávat, že konzistentní právní úpravy a cílevědomá strategie státu navazující na připravovaná opatření Evropské komise v oblasti důvěryhodných služeb umožní vznik efektivní infrastruktury v této důležité oblasti. ICT UNIE je připravena být aktivním účastníkem v tomto procesu.

Tato verze dokumentu neobsahuje přílohy. Jedná se o následující analytické podklady, ze kterých pracovní skupina vycházela při své práci:

1. Rozbor
1.1 Situace v ČR a právní podmínky
1.2 Situace v některých zemích EU
1.3 Právní podmínky EU
2. Přehled českých právních a technických norem
3. Přehled evropských legislativních a technických norem
4. Rešerše

Kompletní verzi dokumentu naleznete na webové stránce ICT UNIE http://www.ictu.cz/.

Na zpracování dokumentu se podíleli členové pracovní skupiny Archivnictví:

Vladimíra Hloušková, Jaroslav Lubas, Ivo Rosol, Boleslav Bobčík

Poznámka autorského kolektivu

Při tvorbě tohoto dokumentu autoři vycházeli ze současné právní úpravy a technických standardů ČR a EU, ze zkušeností a praxe různých členských států EU a také z historických zvyklostí a právních premis.

Autoři si jsou vědomi, že „důvěryhodnost“ konkrétního dokumentu jakožto důkazního prostředku v soudním řízení může určit pouze soud.

Materiál je k dispozici v elektronické podobě na webových stránkách ICT UNIE – **www.ictu.cz**.

ICT UNIE o.s.
K Červenému dvoru 25a/3269
130 00 Praha 3
tel.: +420 222 582 880
fax: +420 222 585 278
info: ictu@ictu.cz
www.ictu.cz