Důvěryhodný digitální dokument

Stanovisko ICT UNIE k problematice právně validního dokumentu

ICT UNIE

Pracovní skupina Archivnictví

Verze dokumentu	
Verze	1.2
Autor	Vladimíra Hloušková, Jaroslav Lubas, Ivo Rosol, Boleslav Bobčík
Datum	25. 3. 2014
Počet stran	58

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.

Obsah

Seznam obrázků

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 Systém (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 identit.
CRL	Certificate revocation list - seznam zneplatněných certifikátů vydávaný 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
Dokument	Podle §2 písm. e) zákona č.499/2004Sb., 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 přijímacích 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[1].
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
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

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

	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.[2]
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.
Omezení rozsahu důvěryhodnosti	Každý dokument prochází určitým životním cyklem, od svého vzniku, používání, autorizované změny, 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 elektronickými 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 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.
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

[2] Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů v platném znění – příloha č. 1.

	skartaci.
Skartační režim	NSESSS[3]: 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 uděleného 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 osoby; za stejnopis se považuje rovněž druhopis, pokud tak stanoví jiný právní předpis.
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 vykoná-ván dohled podle předpisu Evropské unie.
Validace	Ověření integrity dokumentu, kompletnosti metadat a stavu bezpečnostních

[3] VMV čá. 64/2012 (část II), Národní standard pro elektronické systémy spisové služby

	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.

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 jeho zničení.

Definice důvěryhodného digitálního dokumentu

Dokument[4] 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[5];
- 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 dalším zaváděním digitálních dokumentů do praxe řešit.

   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.

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

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

- 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.

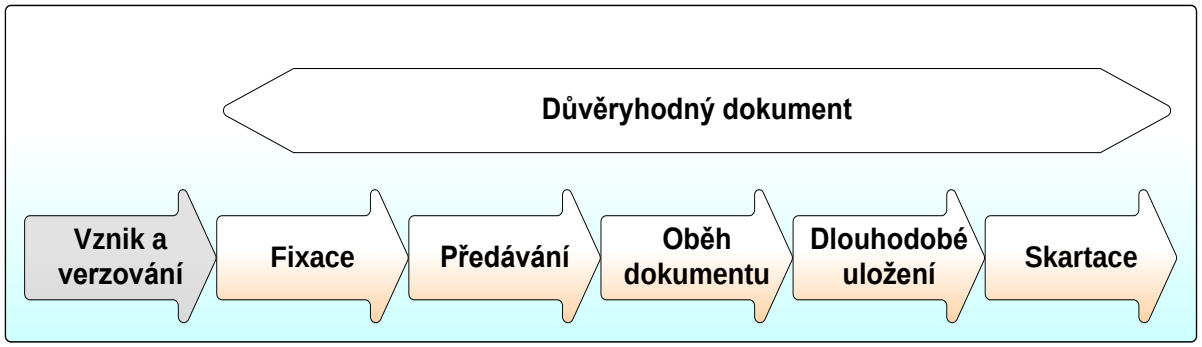
Následně bude tento koncept ze strany ICT UNIE veřejně popularizován.

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. 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 universitu (**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 dokumentů 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

3. Důvěryhodný dokument

3.1. 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.

Vycházeje 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].

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

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).

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.

3.2. 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, které 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.

4. 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 – automatického označování elektronickými značkami a časovými razítky, automatické kontroly 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).

5. 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 s k důkaznímu materiálu definující čas generování důkazního materiálu.

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

6. 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.

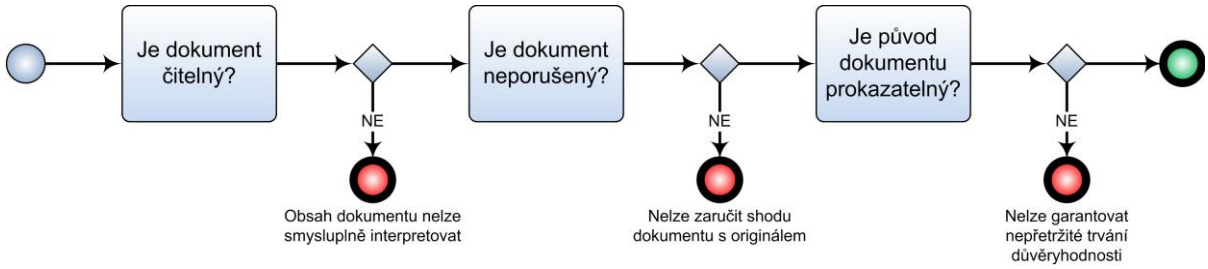
Cílem rozboru různých forem selhání důvěryhodnosti je pomoc při pochopení, na jakých principech je konstrukt „důvěryhodnosti“ či „pravosti“ vystavěn, pomocí jakých prostředků jsou tyto principy prosazovány, jaká jsou jejich inherentní omezení a jak lze tato omezení překonat.

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.



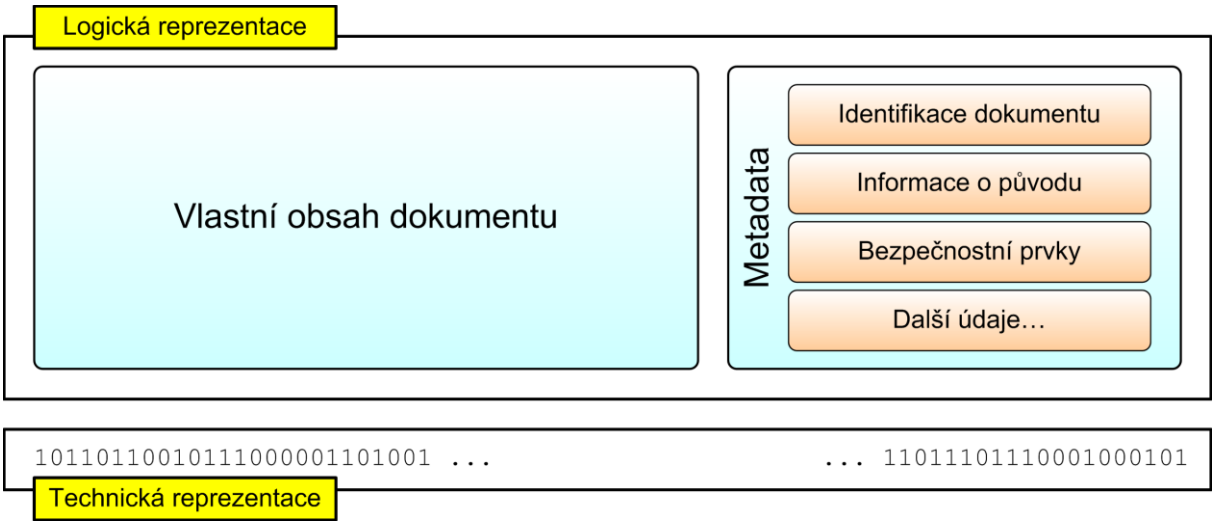
Obrázek 2: Způsob vyhodnocení důvěryhodnosti dokumentu

6.1. 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 Obrázek 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.

6.2. 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.

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

[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.

zohlednit způsob, jakým způsobem je zajištěna jeho integrita jak jednotlivých částí, tak i výsledného celku. Lze konstatovat, že hlavním úkolem soudobých metody 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).

6.3. Původ dokumentu

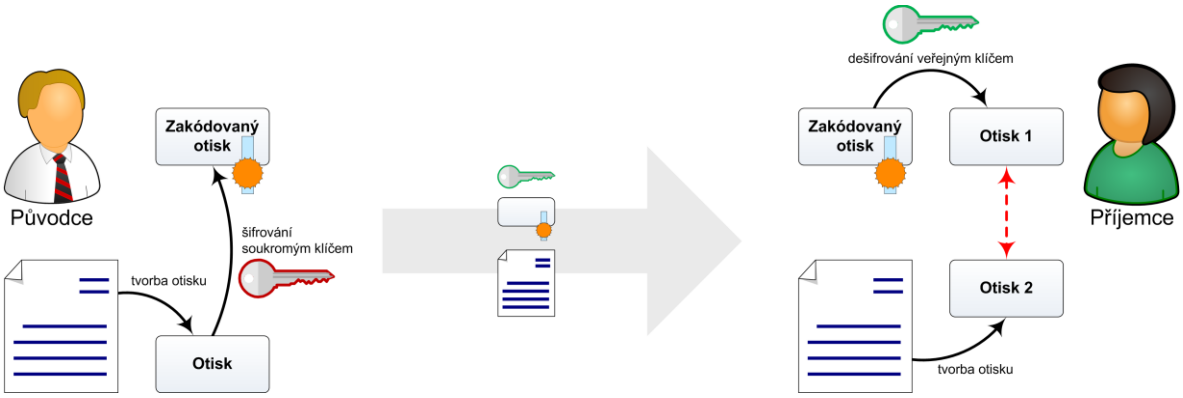
Souhrnné označení „informace o původu dokumentu“ zahrnuje řadu dílčích aspektů. Patří mezi ně:

- 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 6.2, 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 muže 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 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 v důsledku, 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.

7. Navazující aktivity pracovní skupiny ICTU – Archivnictví

7.1. 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 procesním 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 č. 3, 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 elektronického 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 označování 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 k 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“.

7.2. 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 (na doporučení doc. Polčáka osloven JUDr. Tomáš Lichovník, prezident Soudcovské unie, v současné době v řešení)
- Soudní znalci Znaleckého ústavu Apogeo Esteem (vedoucí týmu je manažerem ICT divize Znaleckého ústavu)

První schůzka je plánována na konci března 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.

8. 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.

Přílohy

1. Rozbor

1.1. Situace v ČR a právní podmínky

V České republice neexistuje zákonná definice pro důvěryhodný dokument. Existuje pouze definice, kdy se považuje elektronický dokument za pravý.

Novela zákona o archivnictví a spisové službě (zákon č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony, který upravuje, kromě jiného, klíčový §69a) považuje dokument za pravý „byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“.

Znamená to, že z původního „zaručeného elektronického podpisu“, kdy na původ jeho certifikátu nebyly kladeny zásadní požadavky, dochází ke změně, která s sebou přináší nutnost použití kvalifikovaného certifikátu, který může být vydán jen akreditovanou certifikační autoritou, která navíc ověří identitu osoby, která o elektronický podpis žádá. To znamená, že se vyžaduje použití „uznávaného elektronického podpisu“ nebo „uznávané elektronické značky“. V České republice existují v současné době tři akreditované certifikační autority: První certifikační autorita, a.s. (I.CA), PostSignum a eIdentity. Z tohoto vyplývá, že pro kontrolu, zda elektronický podpis je skutečně uznávaný, musíme ověřit, která certifikační autorita certifikát k elektronickému podpisu vydala.

„Důvěryhodné postupy“ jsou uplatňovány pouze při převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak a změně datového formátu dokumentu v digitální podobě, kterou provádí určený původce postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu.

V případě elektronického podpisu, pocházejícího z jiného státu je situace složitější. Pro usnadnění ověřování certifikátů z jiných členských států Evropské unie provozuje Ministerstvo vnitra webovou aplikaci, která po nahrání certifikátu ve formátu CER, DER, CRT nebo PEM vyhodnotí na základě informací publikovaných v seznamu důvěryhodných certifikačních služeb (TSL) jednotlivých členských států, zda byl tento certifikát vydán jako kvalifikovaný. Neověřuje však jeho validitu. Tuto službu poskytují v České republice pouze komerční subjekty.

Znamená to také, že se do novely zákona o archivnictví prolíná zákon 227/2000 Sb v platném znění (viz kapitola Přehled českých právních a technických norem).

Pokročilejší definice vztahující se k „důvěryhodnosti“ dokumentu, konkrétně k listinnému a elektronickému daňovému dokladu, je použita v zákoně č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů kdy se vyžaduje, aby u daňového dokladu musela být od okamžiku jeho

vystavení do konce lhůty stanovené pro jeho uchovávání zajištěna věrohodnost jeho původu, neporušenost jeho obsahu a jeho čitelnost.

Problémem je však to, že v souladu s principem svobodné volby není jednostranně tímto zákonem řečeno, jakým způsobem tyto tři vlastnosti zaručit, a to od okamžiku vystavení až do konce doby uchování. Zákon pouze uvádí, že zajištění věrohodnosti původu daňového dokladu a neporušenosti jeho obsahu lze dosáhnout prostřednictvím kontrolních mechanismů procesů vytvářejících spolehlivou vazbu mezi daňovým dokladem a daným plněním.

Věrohodnost původu daňového dokladu v elektronické podobě a neporušenost jeho obsahu lze vedle kontrolních mechanismů procesů zajistit také uznávaným elektronickým podpisem, uznávanou elektronickou značkou, nebo elektronickou výměnou informací (EDI), jestliže dohoda o této výměně stanoví užití postupů zaručujících věrohodnost původu a neporušenost obsahu.

Jaké jsou další identifikované problémy:

- V České republice existuje zákon o elektronickém podpisu, ale za současné situace nelze vždy jednoznačně identifikovat podepisující osobu pomocí kvalifikovaného certifikátu
    - Chybí univerzálně použitelný identifikátor držitele certifikátu. V současnosti je identifikátorem desetimístné číslo, toto číslo je dostupné pro ověření identity pouze omezené skupině institucí.
- Neexistuje legislativa pro autentizaci
    - Pro elektronickou komunikaci chybí vhodný identifikátor osoby, který by byl součástí certifikátu a elektronického identifikačního prostředku/dokladu.
    - Neexistuje elektronický identifikační prostředek/doklad – elektronický občanský průkaz nebyl realizován použitelným způsobem.
- Není zaručena dostupnost všech nezbytných validačních dat v dlouhodobém časovém období (více než 25 let)
- Neexistuje legislativa definující kvalifikovanou službu pro ověřování elektronického podpisu
- Není legislativně definována služba dlouhodobého uchovávání dokumentů s garantovanou kvalitou.
- Fikce pravosti je nebezpečný mechanismu, u kterého je v praxi velmi problematické ověřit oprávněnost osoby, která dokument podepsala
- Konvertovaný dokument nemůže nikdy nahradit originál
- Měl by být odstraněn konflikt mezi občanským zákoníkem (i novým, s účinností od 1. 1. 2014) a zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů ohledně fikce pravosti podpisu v případě zaslání dokumentu prostřednictvím ISDS[12].

[12] § 40 odst. 3 zákona č. 40/1964 Sb., občanský zákoník stávající: Písemný právní úkon je platný, je-li podepsán jednající osobou. Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.

§ 561 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, účinný od 1. ledna 2014: K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé.

§ 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů: Úkon učiněný osobou uvedenou v § 8 odst. 1 až 4 nebo pověřenou osobou, pokud k tomu byla pověřena, prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.

1.2. Situace v některých zemích EU

Situace v jednotlivých zemích EU v oblasti uznávání elektronického dokumentu za důvěryhodný je rozdílná. Ačkoliv všechny státy zavedly směrnici č. 1999/93/EC, v jejich národní legislativě je tato směrnice implementována různě. Důsledkem toho je pak odlišné reálné praktické používání a akceptace elektronických dokumentů v jednotlivých zemích. Tento stav následně ovlivnil zamýšlenou podobu společného evropského trhu fungujícího na základech e-procurementu.

Významným prvkem, který významně zasahuje do této oblasti je existence identifikačního průkazu (nebo také občanského průkazu), který umožňuje vytvářet elektronický podpis. V zemích, kde nejsou takovéto identifikační průkazy vydávány, nebývají elektronické dokumenty (s výjimkou komerční sféry) v komunikaci tolik rozšířeny a lidmi akceptovány.

Problematiku samotnou bychom mohli rozdělit do následujících oblastí:

- komunikace mezi státními institucemi,
- komunikace státní správy/samosprávy s občanem,
- komunikace mezi státní správou/samosprávou a komerční organizací,
- komunikace mezi komerčními organizacemi,
- archivace elektronických dokumentů.

Oblast elektronických konvertovaných dokumentů není na úrovni EU nijak právně řešena. Jednotlivé státy mají svá vlastní řešení, povětšinou se však jedná o povinnost vidimace potrzené elektronickým podpisem osoby, která tuto vidimaci prováděla. To znamená, že pojem autorizovaná konverze je v zahraničí fakticky neznámý.

Níže popisujeme aktuální situaci ve vybraných zemích Evropské unie.

Itálie

V Itálii jsou elektronické dokumenty hojně využívány a staly se součástí běžného života. Do státní správy se elektronické dokumenty postupně zaváděly již od roku 1993. V současnosti je hlavním legislativní normou tzv. Digitální správní řád aktualizovaný k 22. 6. 2013.

Za důvěryhodné jsou považovány dokumenty, které vznikly jako elektronické a jsou podepsány kvalifikovaných elektronickým podpisem. Obdobně jsou za platné a důvěryhodné považovány také dokumenty konvertované. Specificky jsou považovány za platné také opisy či výpisy informací z elektronických dokumentů pokud jsou vytvořeny dle pravidel a jsou ověřeny (vidimovány) veřejným činitelem.

Až do konce roku 2012 bylo povinností, aby daňové doklady, pokud jsou vystavovány v elektronické podobě, obsahovali kvalifikovaný elektronický podpis nebo byly ve formátu EDI.

Španělsko

Díky zavedení identifikačních průkazů s kvalifikovaným elektronickým podpisem se postupně rozšiřuje využívání elektronických dokumentů jak v komunikaci mezi občany a státní správou, tak také v komerční oblasti.

Španělská legislativa přesně definuje používání elektronických podpisů a způsob autentizace vůči službám e-governmentu. Královský výnos č. 1671/2009 však pokrývá pouze oblast komunikace se státní správou.

Využívání elektronických dokumentů v komerční oblasti definuje Královský výnos č. 56/2007, který se zabývá jak používáním elektronických faktur, tak také možností obchodovat a uzavírat smlouvy elektronicky za podmínky používání kvalifikovaných elektronických podpisů.

Široce jsou využívány AdES formáty. Ty jsou dokonce některými organizace vyžadovány jako např. The Spanish Confederation of Savings Banks.

Rakousko

V Rakousku je nastavena a silně využívána elektronická komunikace mezi občanem a státní správou/ samosprávou.

Využívání elektronických dokumentů v komerční oblasti se rychle rozšiřuje. Převážná část komunikace mezi komerční sférou a státní správou je dnes také v digitální podobě. Podmínkou je používání kvalifikovaného elektronického podpisu.

V současné době není plně vyřešena oblast dlouhodobého uchovávání elektronických dokumentů. To znamená, že nejsou vytvořena jednoznačná pravidla jak s takovými dokumenty nakládat, aby neztratily svou právní validitu.

Slovensko

Na Slovensku existují jednoznačně definovaná pravidla pro tvorbu důvěryhodného dokumentu, a to jak pro státní sféru, tak i pro komerční organizace.

Nástroje pro tvorbu elektronických podpisů musejí být certifikovány Národním bezpečnostním úradom.

Jako jedna z mála zemí má Slovensko striktně definován způsob nakládání s dokumenty i pro komerční sféru.

Elektronické dokumenty jsou využívány a uznávány v komunikaci (v případě, že jsou podepsány osobním kvalifikovaným elektronickým podpisem):

- v komunikaci mezi občanem a státní správou,
- v komunikaci mezi jednotlivými složkami státní správy/samosprávy,
- v komunikaci mezi komerčními organizacemi a složkami státní správy/samosprávy,
- v komunikaci v komerční sféře.

Dánsko

V rámci severských státu je v rámci zavádění elektronické komunikace s veřejným sektorem nejvíce napřed. Již v současnosti zde existuje systém elektronických identifikačních průkazů obsahující elektronický podpis. Dánské vládě se podařilo digitalizovat veškeré dokumenty a zavést jejich správu, distribuci a publikaci v rámci projektu Public 360$^{o.}$

Od roku 2005 existuje tzv. Electronic mailbox, který umožňuje obyvatelstvu komunikovat s veřejným sektorem elektronicky. Jeho používání je však dobrovolné.

Od roku 2015 by měla být elektronická komunikace mezi občany a veřejným sektorem upřednostněna tím, že bude zaveden tzv. Public sector document box a předpokládá se, že ho bude využívat více než 80% obyvatelstva – tedy téměř všichni obyvatelé starší 15 let.

V Dánsku existuje zákon o elektronickém podpisu a návazné prováděcí předpisy.

V současnosti jsou zaznamenávány problémy s dlouhodobým uchováváním elektronických dokumentů. Z důvodu neexistující legislativy není zajištěna interoperability těchto dokumentů a způsoby uchovávání a dlouhodobé správy se i v rámci veřejného sektoru liší. Jedním z velkých poskytovatelů této služby se stala Dánská pošta projektem eFirst Mailroom.

V komunikaci se státní správou, samosprávou nebo obchodní komunikaci se používá zaručený elektronický podpis založený na kvalifikovaném certifikátu.

Elektronické dokumenty jsou běžně využívány a uznávány (jejich používání je však dosud dobrovolné):

- v komunikaci s místními samosprávami (elektronické žádosti, zápisy do mateřských škol apod.),
- v komunikaci mezi občanem a státní správou,
- v komunikaci v komerční sféře,
- v komunikaci mezi komerčními organizacemi a složkami státní správy/samosprávy.

1.3. Právní podmínky EU

V současné době existují a jsou platné pouze normativy, které mají formu doporučení. Jako zásadní pro definici „Důvěryhodného dokumentu“ lze považovat směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. Díky tomu, že členské státy EU tuto směrnici implementovali odlišným způsobem, nebylo možné do současné doby sjednotit v rámci EU jak způsob tvorby Důvěryhodného dokumenty, tak také jeho uznávání.

Na základě zkušeností se zaváděním výše uvedené směrnice byl zpracován nový normativ č. COM(2012) 238, Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu, který je v současné době v procesu schvalování jednotlivými členskými státy. Předpoklad jeho schválení ze strany Evropského parlamentu je v dubnu 2014. Ten bude nadřazen národním legislativám a měl by tak sjednotit podmínky v rámci e-procurementu celé EU.

Kromě výše uvedených dokumentů, byly v rámci orgánů EU zpracovány také další normativy, které se zabývají buďto specifickými typy dokumentů jako např. elektronickými fakturami, tak také formáty a strukturou elektronických dokumentů.

Seznam platných normativů vydaných orgány EU v oblasti „Důvěryhodného dokumentu“ je uveden v kap. Přehled evropských legislativních a technických norem.

2. Přehled českých právních a technických norem

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
CZ0001	elektronický podpis	electronic signature	Zákon č. 227/2000 Sb., zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu, ve znění pozdějších předpisů	Smyslem zákona o elektronickém podpisu je umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent podpisu vlastnoručního při běžné listinné formě komunikace. Zákon byl vytvořen na základě směrnice Evropské unie 1999/93/EC ze dne 13. 12. 1999.
CZ0002	elektronický podpis	electronic signature	Zákon č. 440/2004 Sb., kterým se mění zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů	Tento předpis nově zavádí pojem „kvalifikované časové razítko“, které prokazuje existenci elektronického dokumentu v čase. Další novinkou je možnost používat „elektronické značky“. Pro ty se stejně jako pro zaručený elektronický podpis používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.
CZ0003	elektronický podpis	electronic signature	Zákon č. 101/2010 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a zákon č. 227/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech, ve znění pozdějších předpisů	Tento předpis v reakci na komitologické rozhodnutí 2009/767/ES přidává Ministerstvu vnitra povinnost vést a zveřejňovat seznam důvěryhodných certifikačních služeb a stanoví orgánům veřejné moci povinnost uznávat kvalifikované certifikáty vydané v ostatních členských státech EU.
CZ0004	elektronický podpis	electronic signature	Zákon č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související	Novela zavádí pojem „uznávaný elektronický podpis“ a „uznávanou elektronickou značku“. V návaznosti na přímo použitelný předpis Evropské unie - „Rozhodnutí Komise 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu“ stanovuje k podepisování nebo označování dokumentu

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
			zákony	v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči státu; územnímu samosprávnému celku; právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem; právnické osobě vykonávající působnost v oblasti veřejné správy (týká-li se dokument této působnosti); fyzické osobě vykonávající působnost v oblasti veřejné správy (týká-li se dokument této působnosti), používat uznávaný elektronický podpis nebo uznávanou elektronickou značku v referenčním formátu stanoveném v Rozhodnutí Komise 2011/130/EU. Rovněž stanovuje postup pro případy, kdy není použit referenční formát. Zákon č. 227/2000 Sb. tak nově ukládá povinnosti i v oblasti používání elektronického podpisu.
CZ0005	elektronický podpis	electronic signature	Vyhláška 212/2012 Sb.	Vyhláška o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)
CZ0006	poskytování certifikačních služeb	Certification Authority	Vyhláška č. 378/2006 Sb.	První část vyhlášky je určena poskytovatelům certifikačních služeb a obsahuje požadavky na jejich postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Druhá část se vztahuje na označující osoby, zejména na orgány veřejné moci – obsahuje požadavky na ochranu soukromých klíčů, které se používají při vytváření elektronických značek.

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
CZ0007	konverze, autorizovaná konverze	conversion	Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění zákona č. 190/2009 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony,	Definuje převod dokumentu mezi papírovou a elektronickou formou
CZ0008	elektronický podpis	electronic signature	Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů	**Společné ustanovení o doručování** § 19 - V případě doručování na elektronickou adresu platí, že písemnost je doručena v okamžiku, kdy převzetí doručované písemnosti potvrdí adresát zprávou opatřenou jeho zaručeným elektronickým podpisem. **Podání** § 37 je možno učinit písemně nebo ústně do protokolu anebo v elektronické podobě podepsané zaručeným elektronickým podpisem. **Náležitosti rozhodnutí** § 69 Pokud se na žádost účastníka má rozhodnutí doručit elektronicky, vyhotoví úřední osoba, která za písemné vyhotovení rozhodnutí odpovídá, jeho elektronickou verzi s tím, že na místě otisku úředního razítka vyjádří tuto skutečnost slovy "otisk úředního razítka" a dokument podepíše svým zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.
CZ0009	elektronický podpis	electronic signature	Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů	předpis byl zrušen - Zákonem č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
CZ0010	elektronický podpis	electronic signature	vyhláška č. 496/2004 Sb., o elektronických podatelnách	Předpis byl zrušen - Zákonem č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony
CZ0011	elektronický podpis	electronic signature	vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby (dále jen „spisová vyhláška“)	Vyhláška č. 191 byla zrušena a nahrazena vyhláškou 259 ze dne 20. 7. 2012 – §6 postupy ověřování platnosti uznávaného elektronického podpisu, kvalifikovaného certifikátu.
CZ012	Konverze	conversion	vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů	Vyhláška upravuje: - technické náležitosti provádění autorizované konverze dokumentů (dále jen „konverze“), - technické náležitosti dokumentu, který provedením konverze vznikl (dále jen „výstup“), - technické náležitosti dokumentu, jehož převedením výstup při konverzi vznikl (dále jen „vstup“), - vzor osvědčení o vykonání zkoušky zaměstnance provádějícího konverzi na žádost.
CZ0013	uchovávání, formáty	preservation, document types	vyhláška č. 194/2009 Sb., o stanovení podrobností užívání informačního systému datových schránek	- ukládání datové zprávy v ISDS 90 dnů - přípustné formáty datové zprávy
CZ0014	dokumenty v digitální podobě, převody	digital documents, conversions	Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,	Původní znění - Zvláštní ustanovení o dokumentech v digitální podobě „§69a (1) Není-li doručený dokument v digitální podobě opatřen uznávaným elektronickým podpisem, elektronickou značkou nebo kvalifikovaným časovým razítkem, určený původce jej opatří kvalifikovaným časovým razítkem. (2) Je-li doručený dokument v digitální podobě opatřen uznávaným elektronickým podpisem, elektronickou značkou nebo kvalifikovaným časovým razítkem, určený původce

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
				a) ověří platnost uznávaného elektronického podpisu, elektronické značky nebo kvalifikovaného časového razítka a platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, b) zaznamená údaje o výsledku ověření podle písmene a) a uchová je spolu s doručeným dokumentem v digitální podobě. (3) Uchovávání dokumentu v digitální podobě provádí určený původce postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost jeho ob- sahu a čitelnost dokumentu, a to včetně údajů prokazujících existenci dokumentu v digitální podobě v čase. Tyto vlastnosti musí být zachovány po dobu skartační lhůty dokumentu. Je-li potřeba zachování věrohodnosti původu dokumentu kratší než skartační lhůta dokumentu, uvede to určený původce ve svém spisovém a skartačním plánu. (4) Převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak a změnu formátu dokumentu v digitální podobě provádí určený původce postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost jeho obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu. (5) Připojení údajů, které vznikly při přípravě dokumentu k uchování podle odstavce 3 nebo při převedení či změně formátu dokumentu podle odstavce 4 a které jsou pro uchování dokumentu nebo převedení či změnu formátu dokumentu nezbytné, se nepovažuje za porušení obsahu dokumentu. (6) Před převedením dokumentu v digitální podobě na dokument v analogové podobě nebo změnou formátu dokumentu v digitální podobě ověří určený původce platnost uznávaného elektronického podpisu, elektronické značky nebo kvalifikovaného časového razítka, je-li jimi dokument v digitální podobě opatřen. Údaje o výsledku ověření a datum převedení dokumentu v digitální podobě na dokument v analogové podobě nebo datum změny formátu dokumentu v digitální podobě určený původce zaznamená a uchová je spolu s dokumentem vzniklým

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
				převedením nebo změnou formátu. (7) Dokument v digitální podobě vzniklý převedením z dokumentu v analogové podobě nebo změnou formátu dokumentu v digitální podobě doplněný o datum převedení opatří určený původce uznávaným elektronickým podpisem osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě, nebo svojí elektronickou značkou a kvalifikovaným časovým razítkem. (8) Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentů a opatřen kvalifikovaným časovým razítkem. Ustanovení věty první se vztahuje i na dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“.
CZ0015	dokumenty v digitální podobě, převody	digital documents, conversions	Zákon č. 167/2012 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony	„§ 69a (1) Převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak a změnu datového formátu dokumentu v digitální podobě provádí určený původce postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu. (2) Připojení údajů, které vznikly při přípravě dokumentu k uchování podle § 3 odst. 4 nebo při převedení či změně datového formátu dokumentu podle odstavce 1 a které jsou pro uchování dokumentu nebo převedení nebo změnu datového formátu dokumentu nezbytné, se nepovažuje za nezajištění neporušitelnosti obsahu dokumentu. (3) Před převedením dokumentu v digitální podobě na dokument v analogové podobě nebo změnou datového formátu dokumentu v digitální podobě ověří určený původce platnost uznávaného elektronického podpisu, uznávané elektronické značky nebo kvalifikovaného časového razítka, je-li jimi dokument v digitální podobě opatřen, a platnost

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
				kvalifikovaných certifikátů, na kterých jsou založeny. Údaje o výsledku ověření a datum převedení dokumentu v digitální podobě na dokument v analogové podobě nebo datum změny formátu dokumentu v digitální podobě určený původce zaznamená a uchová je spolu s dokumentem vzniklým převedením nebo změnou formátu (4) Dokument v digitální podobě vzniklý převedením z dokumentu v analogové podobě nebo změnou formátu dokumentu v digitální podobě opatří určený původce doložkou, která ob- sahuje údaje týkající se převedení nebo změny datového formátu, podepsanou uznávaným elektronickým podpisem osoby odpovědné za převedení z dokumentu v analogové podobě anebo změnu datového formátu dokumentu v digitální podobě nebo označenou elektronickou značkou určeného původce, a dále opatřenou kvalifikovaným časovým razítkem Údaje týkající se převedení nebo změny datového formátu stanoví prováděcí právní předpis. Prováděcí právní předpisy stanoví podrobnosti struktury spisového plánu, údaje záznamu o ověření autentizačních prvků, údaje doložky o převodu dokumentu, postup ověřování elektronického podpisu/značky a časového razítka (5) Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným-uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“. - upravena definice uznávaného elektronického podpisu – již neplatí

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
				„zaručený elektronický podpis“ nebo „elektronický podpis založený na ...“, ale nově je definován termín „uznávaný elektronický podpis“. Obdobně „uznávanou elektronickou značkou“ se rozumí elektronická značka založená na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.
CZ0016	elektronický podpis, stejnopis	electronic signature, duplication	Vyhláška č. 259 /2012 Sb., o podrobnostech výkonu spisové služby	§6 - postupy ověřování platnosti uznávaného elektronického podpisu, kvalifikovaného certifikátu §16 - Prvopisem je originální dokument zaznamenávající projev vůle osoby, který je osvědčen jejím vlastnoručním podpisem nebo obdobným autentizačním prvkem stanoveným jiným právním předpisem13). 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 předpis14). Druhopisem je dokument odvozený od prvopisu, se kterým je obsahově shodný, avšak projev vůle osoby obsažený v druhopisu není osvědčen podpisem této osoby, ale vlastnoručním podpisem nebo obdobným autentizačním prvkem osoby stanovené jiným právním předpisem, popřípadě zvláštním autentizačním prostředkem stanoveným jiným právním předpisem.
CZ0017	metadatový model, evidence dokumentů		Věstník MV čá. 64/2012 Národní standard pro elektronické systémy spisové služby	Novelizaci národního standardu pro elektronické systémy spisové služby. V textu byly odstraněny nedostatky, na které upozornili původci a obchodní společnosti zabývající se vývojem elektronických systémů spisové služby. Především šlo o provedení oprav v modelu vztahů mezi entitami, o terminologické změny vycházející z novely zákona č. 499/2004 Sb. (včetně pojmu „Typový spis“) a nahrazení metadatového modelu souborem většího počtu upřesněných schémat XML umožňující praktickou aplikaci jednotlivých požadavků.

ID	Název oblasti v ČJ	Název oblasti v AJ	Název právní či technické normy	Citace, definice
CZ0018	záznam, elektronický podpis	record, digital signiture	Zákon č. 353/2001 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a některé další zákony	Novela zákona č. 563/1991 Sb., o účetnictví obsahující definici účetního dokladu § 33a Průkaznost účetního záznamu odst. 3: Účetní záznam určený k přenosu musí být podepsán vlastnoručním podpisem nebo uznávaným elektronickým podpisem podle zvláštního právního předpisu (zákon č. 227/2000 Sb., o elektronickém podpisu v posledním znění) anebo obdobným průkazným účetním záznamem v technické formě. Pokud účetní záznam není podepsán před předáním k přenosu, musí být podepsán nejpozději v okamžiku jeho předání k přenosu.
CZ0019	elektronický dokument – faktura, dlouhodobé uchovávání, konverze	electronic document, invoice longterm preservation, conversion	Zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů	viz. Doporučení NF-ELFA při HK k novele DPH 2012 - tři vlastnosti daňového dokladu formulované v § 34, v oddíle 7 o zajištění věrohodnosti původu, neporušenosti obsahu a čitelnosti daňových dokladů - stejné požadavky kladeny na listinnou formu - Zajištění věrohodnosti původu daňového dokladu a neporušenosti jeho obsahu lze dosáhnout prostřednictvím kontrolních mechanismů procesů vytvářejících spolehlivou vazbu mezi daňovým dokladem a daným plněním. - Věrohodnost původu daňového dokladu velektronické podobě a neporušenost jeho obsahu lze vedle kontrolních mechanismů procesů zajistit také uznávaným elektronickým podpisem, uznávanou elektronickou značkou, nebo elektronickou výměnou informací (EDI), jestliže dohoda o této výměně stanoví užití postupů zaručujících věrohodnost původu a neporušenost obsahu.
CZ0020	elektronický podpis	digital signiture	Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů	zasílání dokumentů v elektronické podobě, elektronický podpis

3. Přehled evropských legislativních a technických norem

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
E0001	elektronický dokument	electronic document	Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. Prosince 1999 o zásadách Společenství pro elektronické podpisy, (21)	Aby došlo k obecnému přijetí metod elektronického ověřování pravosti, je nezbytné zajistit, aby elektronické podpisy mohly být ve všech členských státech používány jako důkazy v soudním řízení. Právní uznání elektronických podpisů by mělo být založeno na objektivních kritériích a nemělo by záviset na povolení dotčených ověřovatelů. Vnitrostátní právní předpisy vymezí právní oblasti, ve kterých lze používat elektronické dokumenty a elektronické podpisy. Touto směrnicí nejsou dotčeny pravomoci vnitrostátního soudu rozhodovat o souladu s požadavky této směrnice ani vnitrostátní předpisy o volném právním hodnocení důkazů.
E0002	elektronický podpis, elektronický dokument	electronic signature	Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. Prosince 1999 o zásadách Společenství pro elektronické podpisy	1. „elektronickým podpisem“ údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti; 2. „zaručeným elektronickým podpisem“ elektronický podpis, který splňuje tyto požadavky: a) je jednoznačně spojen s podepisující osobou, b) umožňuje zjistit totožnost podepisující osoby, c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou, a d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoli následnou změnu těchto dat;
E0003	elektronický podpis	electronic signatures	European Committee for Standardization: Guide on the Use of Electronic Signatures – Part 1: Legal and Technical Aspects,CWA 14365-1	42 rit laid down in article 5.1 that electronic signatures fulfilling certain quality metrics – so called qualified electronic signatures – satisfy the requirements of handwritten signatures. In article 5.2 a residual provision is given where electronic signatures are not denied legal effectiveness and admissibility as evidence in legal proceedings, even if the quality

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				metrics of qualified electronic signatures are not met.
E0004	elektronický dokument	electronic document	Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu, 2012/0146 (COD) / COM(2012) 238 final, Oddíl 6 Elektronické dokumenty, Článek 34 Právní účinky a přijímání elektronických dokumentů	1. Elektronický dokument se považuje za rovnocenný dokumentu v papírové podobě a je přípustný jako důkaz v soudním řízení, pokud jde o záruku jeho pravosti a integrity. 2. U dokumentu opatřeného kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou značkou osoby, která je oprávněna k vydání příslušného dokumentu, platí právní domněnka jeho pravosti a integrity, pokud dokument neobsahuje dynamické prvky, které mohou dokument automaticky změnit. 3. Vyžaduje-li se při poskytování internetové služby nabízené subjektem z veřejného sektoru originální dokument nebo ověřená kopie, uznávají se v ostatních členských státech bez dodatečných požadavků alespoň elektronické dokumenty, které jsou vydány osobami oprávněnými k vydávání příslušných dokumentů a které se podle vnitrostátních právních předpisů členského státu původu považují za originály nebo ověřené kopie. 4. Komise může stanovit formáty elektronických podpisů a značek, které jsou přijímány, pokud členský stát požaduje pro poskytnutí internetové služby nabízené subjektem z veřejného sektoru dokument opatřený podpisem nebo značkou uvedený v odstavci 2, prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.
E0005	elektronický dokument	electronic document	Rozhodnutí komise č. K(2011) 1081 ze dne 25. Února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského	1. Členské státy zavedou nezbytné technické prostředky, které jim umožní zpracování elektronicky podepsaných dokumentů, jež v rámci plnění postupů a formalit předkládají poskytovatelé služeb prostřednictvím jednotných kontaktních míst, jak je stanoveno v článku 8 směrnice 2006/123/ES, a které jsou podepsány příslušnými orgány jiných členských států pomocí zaručeného elektronického podpisu XML nebo

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
			parlamentu a Rady o službách na vnitřním trhu, Článek 1 Referenční formát elektronických podpisů	CMS nebo PDF ve formátu BES nebo EPES, který je v souladu s technickými specifikacemi uvedenými v příloze. 2. Členské státy, jejichž příslušné orgány podepisují dokumenty uvedené v odstavci 1 za použití jiných formátů elektronických podpisů, než jsou uvedeny v odstavci 1, oznámí Komisi stávající možnosti ověření, které umožní ostatním členským státům ověřit obdržené elektronické podpisy online, bez poplatku a způsobem, který je srozumitelný pro nerodilé mluvčí, pokud požadované informace nejsou již zahrnuty v dokumentu, elektronickém podpise nebo nosiči elektronického dokumentu. Komise zpřístupní tyto informace všem členským státům.
E0006	elektronický dokument	electronic document	E-invoices and digital signatures, CWA 15579	This CWA summarizes findings and issues identified by the e-Invoicing Focus Group set up by CEN/ISSS regarding electronic invoicing using electronic signatures. Issues surrounding electronic signatures relating to e-Invoicing and VAT in relation to the Council Directive 2001/115/EC are covered, which had to be implemented by Member States by 1st January 2004. Council Directive 2001/115/EC, details the requirements on taxable persons and their service providers to guarantee the integrity and the authenticity of electronic invoices for VAT purposes. Electronic signatures are a valuable technique to ensure the integrity and authenticity of electronic business data such as invoices. This value, which is based on electronic signatures – under certain conditions providing integrity and authenticity assurances regardless of time and type of electronic (transport or storage) medium, has been recognized within the EU through the e-Signature Directive, as well as more recently through Council Directive 2001/115/EC where they are one of a limited set of compliance options for sending and storage of electronic invoices.
E0007	Elektronický dokument	electronic document	eInvoice Reference Model for EU VAT purposes specification, CWA 15582	The present document specifies the eInvoicing Reference model, which describes the eInvoicing processes: - the business functions between the parties involved in electronic invoicing; - the processes of V.A.T. declaration and verification; - the electronic business services to support the eInvoicing. The present document is applicable to the 44 rit44 of

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				electronic invoicing in the European Union, in line with Council Directive 2001/115/EC. The Reference Model includes and refers to the other tasks from the eInvoicing CEN Workshop. This CWA describes the eInvoicing Reference Model, 45 rit4545r by the e-Invoicing Focus Group set up by CEN/ISSS regarding electronic invoicing. The Reference Model covers modelling issues relating to e-Invoicing and VAT in relation to the Council Directive 2001/115/EC, which had to be implemented by Member States by 1st January 2004. Council Directive 2001/115/EC, details the requirements on taxable persons and their service providers to guarantee the integrity and the authenticity of the of electronic invoices for VAT purposes. The Reference Model aims to describe the business processes involved in ©Invoicing, including the business relations, the processes required for the VAT 45 rit45, and the processes for the eBusiness services for the 45 rit4545r of eInvoices between supplier and customer. The Reference Model gives a full overview of the processes so as to put the VAT Directive in the context of the 45 rit45 ©Invoicing actions. The final review/endorsement round
E0008	konverze elektronického dokumentu	conversion	eInvoice Reference Model for EU VAT purposes specification, CWA 15582, 4.3.2 CONVERSION	Electronic invoice data are converted (e.g. into another 45 rit4545r using another protocol) to allow for the eInvoice processing between Customer and Supplier. The original file of the invoice is stored in accordance with the national and EU legislation.
E0009	autenticita	authentication	eInvoice Reference Model for EU VAT purposes specification, CWA 15582, 4.3.4 AUTHENTICATION	The eInvoices are authenticated, for which a Trusted Third party may be used. The authenticity of the origin of the invoice can be guaranteed by either • an advanced electronic signature, or/and • electronic data interchange (EDI).

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
E0010	ukládání, archivace	storage	eInvoice Reference Model for EU VAT purposes specification, CWA 15582, 4.3.8 STORAGE	The eInvoice is stored for accounting purposes, and in accordance with national and EU legislation. Both the Customer and Supplier store a copy of the invoice. The authenticity of the origin and integrity of the content of the invoice, must be guaranteed throughout the storage period. Issues that have to be dealt with are: • the location of the storage • the duration of the storage • the format in which the invoice is stored
E0011	elektronický dokument	electronic document	Electronic invoicing – Part 2: Model Interoperability Agreement for Transmission and Processing of Electronic Invoices and other Business Documents, CWA 16464-2,	Electronic Business Documents means documents or Data in electronic formats that are related to the processes of ordering, procuring shipping, invoicing and paying, but not the actual payment itself. Electronic Business Documents excludes the actual E-Invoice itself, defined elsewhere, and all their associated acknowledgements.
E0012	elektronický dokument, elektronický podpis	electronic document, digital signatures	Electronic invoicing – Part 2: Model Interoperability Agreement for Transmission and Processing of Electronic Invoices and other Business Documents, CWA 16464-2, 9 Conversion, Electronic Signature Validation and Archiving	The Agreement sets out the terms and conditions for the transmission and processing of e-Invoices and other Electronic Business Documents between the Parties for the purpose that their 46 rit4646r e Customers, whether a Sender or a Receiver, shall be able to 46 rit4646r these documents between each other automatically and without manual intervention. The e-Invoices and Electronic Business Documents to be exchanged and such other services as might be mutually agreed will be specified in the Description of Services. Either or both of SP-X or SP-Y may act in the capacity of Sending Party and Receiving Party when performing Services under this Agreement. 9.1 Conversion If the Receiving Party 46 rit46 Receiver undertakes format conversion then such Party is responsible for doing so in compliance with any applicable VAT or other legal requirements. The Sending Party is not responsible for any non-compliance with VAT requirements arising from such conversion. If a Party's Customer requires conversion of the E-Invoices or Electronic Business Documents into another Format Standard

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				or requires transmission through the use of another Transmission Protocol, then such Party and the Customer is responsible for all costs associated therewith, and for ensuring that the conversion is performed correctly in accordance with approved Maps [[optional] and in a manner that satisfies "business control" requirements of Draft Directive 2010/10858/10]. The Parties, to the extent permitted by law, shall treat a properly converted invoice as the equivalent to the original invoice. 9.2 Electronic Signature Validation If separately agreed and set forth in the Description of Services, the Receiving Party, acting for the Receiver of an E-Invoice or Electronic Business Documents, may provide validation of an electronic signature attached to an E-Invoice or Electronic Business Documents received from the Sending Party, either on the basis that the Receiving Party itself performs a validation check on the electronic signature, or on the basis that the Receiving Party receives a validation from the Sending Party (or both). 9.3 Archiving of invoice and other business documents If separately agreed and set forth in the Description of Services, the Sending Party, acting for the Sender of the E-invoice or Electronic Business Documents and 47 rit47 Receiving Party, acting for the Receiver of an E-invoice or Electronic Business Documents, may be contracted to archive the invoices and other required business documents, electronic or on paper, compliant to the legal requirements of the Member States relevant to the transactions.
E0013	elektronický dokument, elektronický podpis	electronic document, digital signatures	European Committee for Standardization: E-invoices and digital signatures, CWA 15579	Electronic signatures play a major role in electronic invoicing – for transmission of invoice data by EDI or non-EDI – to guarantee authenticity of the origin and integrity of the contents of the invoices. Member States may ask for advanced electronic signature to be based on a qualified certificate. In this document questions regarding the adoption of electronic signatures for electronic invoicing are discussed. It should help the reader to implement and integrate its software or hardware

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				solutions for signing and verifying its e-invoices regarding the legal requirements.
E0014	elektronický podpis, identifikace a autorizace osoby	identification, authentication	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu / COM/2012/0238 final - 2012/0146 (COD) }	‘electronic identification’ means the 48 rit48 of using person identification data in electronic form unambiguously representing a natural or legal person; ‘authentication’ means an electronic 48 rit48 that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;
E0015	elektronický dokument	electronic document	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu /COM/2012/0238 final - 2012/0146 (COD) Oddíl 6 Elektronické dokumenty, Článek 34	„Elektronickým dokumentem“ se rozumí dokument v elektronické podobě; Právní účinky a přijímání elektronických dokumentů: 1. Elektronický dokument se považuje za rovnocenný dokumentu v papírové podobě a je přípustný jako důkaz v soudním řízení, pokud jde o záruku jeho pravosti a integrity. 2. U dokumentu opatřeného kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou značkou osoby, která je oprávněna k vydání příslušného dokumentu, platí právní domněnka jeho pravosti a integrity, pokud dokument neobsahuje dynamické prvky, které mohou dokument automaticky změnit. 3. Vyžaduje-li se při poskytování internetové služby nabízené subjektem z veřejného sektoru originální dokument nebo ověřená kopie, uznávají se v ostatních členských státech bez dodatečných požadavků alespoň elektronické dokumenty, které jsou vydány osobami oprávněnými k vydávání příslušných dokumentů a které se podle vnitrostátních právních předpisů členského státu původu považují za originály nebo ověřené kopie. 4. Komise může stanovit formáty elektronických podpisů a značek, které

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				jsou přijímány, pokud členský stát požaduje pro poskytnutí internetové služby nabízené subjektem z veřejného sektoru dokument opatřený podpisem nebo značkou uvedený v odstavci 2, prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.
E0016	elektronický dokument	electronic document	COMMISSION DECISION of 7 July 2004 amending its Rules of Procedure (2004/563/EC, Euratom	Article 4 Validity of electronic documents 1. Whenever the applicable Community or national provision requires the signed original of a document, an electronic document drawn up or received by the Commission satisfies this requirement if the document in question bears an advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device electronic signature offering equivalent assurances with regard to the functionalities attributed to a signature. 2. Whenever the applicable Community or national provision requires a document to be drawn up in writing without, however, requiring a signed original, an electronic document drawn up or received by the Commission satisfies this requirement if the person from whom it emanates is duly identified and the document is drawn up under such conditions as to guarantee the integrity of its contents and of the relevant metadata and is stored in accordance with the conditions laid down in Article 7. 3. The provisions of this Article shall apply from the day following the adoption of the implementing rules referred to in Article 9.
E0017	elektronický dokument	electronic document	IMPLEMENTING RULES FOR THE DECISION 2002/47/EC,ECSC,EURATOM ON DOCUMENT MANAGEMENT AND FOR THE DECISION 2004/563/EC,EURATOM ON	Only born-digital documents can be signed by means of an electronic signature. Article 4(1) is about signing as a substantial formality, a situation in which only the advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device is acceptable as it meets the same requirements (authenticity, non-repudiation and

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
			ELECTRONIC AND DIGITISED DOCUMENTS, SEC(2009)1643, III.2.1.1. General principles	integrity) and has the same legal effects as a handwritten signature, in accordance with Article 5 of Directive 1999/93/EC. As far as possible, the Commission uses the same type of electronic signature, whatever circle is concerned, or interoperable systems that are transparent for the final user. The use of an advanced electronic signature within the Commission does not affect the rules of competence under which the signatory is or is not empowered to take decisions binding on the Commission.
E0018	elektronický dokument	electronic document	IMPLEMENTING RULES FOR THE DECISION 2002/47/EC,ECSC,EURATOM ON DOCUMENT MANAGEMENT AND FOR THE DECISION 2004/563/EC,EURATOM ON ELECTRONIC AND DIGITISED DOCUMENTS, SEC(2009)1643, III.2.1.2. Principles of management of electronic documents drawn up by the Commission and signed by means of an advanced electronic signature	Within the Commission, the Directorate-General for Informatics, assisted by the "Security" Directorate83, is putting in place the technical infrastructure and secure devices required for the creation and utilisation of a public key infrastructure in accordance with the rules of Community law governing electronic signatures, in particular Directive 1999/93/EC. Secure signature-creation devices84 must, by appropriate technical and procedural means, ensure at the least that: (a) the signature-creation-data used can in practice occur only once and their secrecy is reasonably assured; (b) the signature-creation-data used cannot, with reasonable assurance, be derived and the 50 rit5050r eis protected against forgery by the most advanced technology available; (c) the signature-creation-data used can be reliably protected by the legitimate signatory against use by others. In addition secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature 50 rit50. As regards certification services85, either the Commission performs these functions itself 50 rit concludes a contract with an external certification-serviceprovider.
E0019	Elektronický dokument		Codice dell'amministrazione digitale, CAD - Decreto Legislativo 7 marzo 2005, n. 82, Testo vigente dal 22/06/2013 Articolo 21.	Documento informatico sottoscritto con firma elettronica. (65) 1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				e immodificabilità. (66) 2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all' articolo 20, comma 3 , che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. (67) 2-bis. Salvo quanto previsto dall' articolo 25 , le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale. (68) 3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate. 4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni: a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro; b) il certificato qualificato è garantito da un certificatore stabilito nella

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				Unione europea, in possesso dei requisiti di cui alla medesima direttiva; c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali. 5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.
E0020	Smlouva v elektronické formě	Electronic contract	Directive 2000/31/CE of the European Parliament and Council, of 8 June 2000, with regards to certain legal aspects of information society's services, in particular electronic commerce in the interior market (Directive on electronic commerce), (34)	Each Member State is to amend its legislation containing requirements, and in particular requirements as to form, which are likely to curb the use of contracts by electronic means; the examination of the legislation requiring such adjustment should be systematic and should cover all the necessary stages and acts of the contractual process, including the filing of the contract; the result of this amendment should be to make contracts concluded electronically workable; the legal effect of electronic signatures is dealt with by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(24); the acknowledgement of receipt by a service provider may take the form of the on-line provision of the service paid for.
E0021	Elektronický podpis	Electronic signature	Lov om elektroniske signaturer	Elektronisk signatur: Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.
E0022	Elektronický podpis	La firma electrónica	Law 59/2003 of 19 December, an electronic signature (BOE n º 304, 20/12/2003)	La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
E0023	Zaručený elektronický podpis	La firma electrónica avanzada	Law 59/2003 of 19 December, an electronic signature (BOE n º 304,	La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
			20/12/2003)	que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
E0024	Elektronický dokument	El documento electrónico	Law 59/2003 of 19 December, an electronic signature (BOE n º 304, 20/12/2003)	4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel. 5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable. *Número 5 del artículo 3 redactado por el apartado uno del artículo 5 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información («B.O.E.» 29 diciembre).Vigencia: 30 diciembre 2007* 6. El documento electrónico será soporte de: a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso. b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica. c) Documentos privados. 7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable. 8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica. La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil. *Número 8 del artículo 3 redactado por el apartado dos del artículo 5 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información («B.O.E.» 29 diciembre).Vigencia: 30 diciembre 2007* 9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica. 10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.
E0025	Elektronický podpis	Elektronische Signatur	Austrian Signature Act	Elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen;

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
E0026	Zaručený elektronický podpis	Fortgeschrittene elektronische Signatur	Austrian Signature Act	Fortgeschrittene elektronische Signatur: eine elektronische Signatur, die a) ausschließlich dem Signator zugeordnet ist, b) die Identifizierung des Signators ermöglicht, c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann, sowie d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann;
E0027	Kvalifikovaný zaručený podpis	Qualifizierte elektronische Signatur	Austrian Signature Act	Qualifizierte elektronische Signatur: eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird;
E0028	Elektronický podpis	Elektronický podpis	Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, § 3	(1) Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky: a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu, b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie. (2) Podpisovateľ vyhotoví elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj, ktorý spĺňa podmienky podľa odseku 1
E0029	Zaručený elektronický podpis	Zaručený elektronický podpis	Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, § 3	Zaručený elektronický podpis je elektronický podpis, ktorý musí spĺňať podmienky podľa § 3: a) je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu, b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu podľa § 2 písm. h), c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická

ID	Název oblasti v ČJ	Název oblasti v AJ nebo původním jazyce	Název zahraniční/evropské právní či technické normy	Citace, definice
				osoba zaručený elektronický podpis vyhotovila, d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát. (2) Zaručený elektronický podpis je platný, ak a) existuje kvalifikovaný certifikát verejného kľúča patriaceho k súkromnému kľúču použitému při vyhotovení daného elektronického podpisu, b) je preukázateľné, že kvalifikovaný certifikát podľa písmena a) bol platný v čase vyhotovenia daného elektronického podpisu, c) elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie, čo sa overilo použitím verejného kľúča uvedeného v kvalifikovanom certifikáte podľa písmena a). (3) Podpisovateľ vyhotoví zaručený elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a daného elektronického dokumentu vyhotoví pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu nový údaj, ktorý spĺňa podmienky podľa odseku 1. (4) Formát a spôsob vyhotovovania zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad. (5) Verejný kľúč patriaci k súkromnému kľúču určenému na vyhotovovanie zaručeného elektronického podpisu úradu je zverejnený spôsobom, ktorý ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad. (6) Zaručený elektronický podpis úradu je platný, ak elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie, čo sa overilo použitím verejného kľúča úradu zverejneného spôsobom podľa odseku 5

4. Rešerše

Rešerše obsahuje další zdroje pojednávající o důvěryhodném dokumentu a způsobech zajišťujících udržitelnost jeho právní validity.

1. *Australasian Digital Recordkeeping Initiative.* (nedatováno). Načteno z ADRI: http://www.adri.gov.au/

2. Barrister, S. M. (nedatováno). *PROOF OF THE AUTHENTICITY OF A DOCUMENT IN ELECTRONIC FORMAT INTRODUCED AS EVIDENCE.* Načteno z ARMA International Educational Foundation: http://www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/Proof_of_authenticity_of_a_document.pdf

3. Cimander, R., Hansen, M., & Kubicek, H. (červen 2009). *Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe. Lessons from the PROCURE-project.* Načteno z https://www.eid-stork.eu/dmdocuments/public/ElectronicSignaturesAsObstaclesForCross-BorderEProcurementInEurope_LessonsFromThePROCUREProject.pdf

4. Digman, B. (nedatováno). *Electronic Signatures and Records Act (ESRA).* Načteno z ITS (Office of Information Technology Services): http://www.its.ny.gov/policy/esra/esra.htm

5. Gliniecki, J., & Ogada, C. (nedatováno). *Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce.* Načteno z http://scholarlycommons.law.northwestern.edu/njilb/vol13/iss1/10/

6. Information and record management society, Czech Republic. (2012). *Správa dokumentů, Slovník pojmů.* Načteno z http://www.irms.cz/sqlcache/2013-08-30-irms-slovnik-print.pdf

7. *InterPARES Project.* (nedatováno). Načteno z InterPARES: http://www.interpares.org/book/

8. *Modular Requirements for Records Systems.* (nedatováno). Načteno z http://moreq2010.eu/

9. *Podmínky důvěryhodnosti elektronických dokumentů v archivu.* (nedatováno). Načteno z DigiArchiv.eu – projekt MI ČR 2007: http://digiarchiv.eu/dokumenty/zprava/cast2a.pdf

10. *Recommendation on the Legal Value of Computer Records.* (nedatováno). Načteno z UNCITRAL(United Nations Commission on International Trade Law): http://www.uncitral.org/uncitral/en/index.html