Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Informační systémy ve veřejné správě – elektronická spisová služba

Jana KULHÁNKOVÁ

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jana Kulhánková

Veřejná správa a regionální rozvoj – c.v. Litoměřice

Název práce

Informační systémy ve veřejné správě – elektronická spisová služba

Název anglicky

Information Systems in Public Administration – Electronic Filing Service

---

Cíle práce

Analyzovat současný stav informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby a navrhnout alternativní řešení odlišná od současného stavu.
Dílčím cílem je identifikace částí Národního standardu pro elektronické systémy spisové služby, které jsou z pohledu orgánů veřejné moci nadbytečné.

Metodika

Teoretická část: Analýza současného právního rámce informačních systémů ve veřejné správě.

Rešerše zákonů a odborné literatury ve státní správě, popis a zhodnocení současného stavu.

Praktická část: Analýza současného stavu informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby jako páteřního systému.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Digitální technologie, informační systém veřejné správy, elektronická spisová služba, podniková architektura informačních systémů, Národní standard pro elektronické systémy spisové služby, veřejná správa, orgán veřejné moci, eGovernment.

Doporučené zdroje informací

BROM, B. Spisová a archivní služba ve veřejném a soukromém sektoru: praktická příručka pro správu dokumentů. Praha: Linde Praha, 2013. 319 s. ISBN 978-80-7201-913-7

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. KATEDRA INFORMAČNÍCH TECHNOLOGIÍ. *Aspekty a trendy současného rozvoje ICT. II, Kancelář on-line.* V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2021. ISBN 978-80-213-3096-2.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. KATEDRA INFORMAČNÍCH TECHNOLOGIÍ. *Aspekty a trendy současného rozvoje ICT. I.* V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2021. ISBN 978-80-213-3094-8.

DONÁT, J., MAISNER, M., PIFFL, R. Nařízení eIDAS: Komentář. Praha: C.H. Beck, 2017. 283 s. ISBN 978-80-7400-633-3

KUNT, M., LECHNER, T. Spisová služba. 2. aktual. vyd. Praha: Leges, 2017. 384 s. ISBN 978-80-7502-233-2

LECHNER, Tomáš. *Elektronické dokumenty v právní praxi.* Praha: Leges, 2013. ISBN 978-80-87576-41-0.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 2. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 10. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Informační systémy ve veřejné správě – elektronická spisová služba" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 20. listopadu 2023 _____

Poděkování

Ráda bych touto cestou poděkovala Mgr. Ing. Vladimíru Očenáškovi, Ph.D. za odborné metodické vedení při zpracování práce, cenné rady, podněty a připomínky.

Informační systémy ve veřejné správě – elektronická spisová služba

Abstrakt

Diplomová práce se zabývá analýzou informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby jako páteřního systému. Analyzuje novelizace stěžejních legislativních předpisů a zavedení povinných atestací dle Národního standardu pro elektronické systémy spisové služby. Na zvolených příkladech ukazuje, jak jsou řešeny u konkrétního veřejnoprávního původce a uvádí příklady, kdy jsou atestační požadavky vycházející z Národního standardu pro elektronické systémy spisové služby z pozice veřejnoprávního původce nadbytečné.

Klíčová slova: Digitální technologie, informační systém veřejné správy, elektronická spisová služba, podniková architektura informačních systémů, Národní standard pro elektronické systémy spisové služby, veřejná správa, orgán veřejné moci, eGovernment.

Information Systems in Public Administration – Electronic Filing Service

Abstract

This thesis focuses on the analysis of information systems in public administration, with specific focus being laid on the issue of the electronic records service as a core system. It analyzes amendments to key legislative regulations and the introduction of mandatory certifications, as set by the National Standard for electronic record service systems. Using selected examples, it demonstrates how specific public authorities address these issues and provides examples where certification requirements stemming from the National Standard for electronic record service systems are deemed redundant from the perspective of public authorities.

Keywords: Digital technology, public administration information system, electronic records service, enterprise architecture of information systems, National Standard for electronic record service systems, public administration, public authority, eGovernment

Obsah

1 Úvod

Spisovou službu je možno datovat hluboko do historie, a to proto, že jejím předmětem jsou úřední dokumenty, které bylo nutné dlouhodobě zachovat. Dokumenty obsahují informace. Informace vždy byly, jsou a budou zaznamenávány, evidovány, tříděny, zpracovávány a uchovávány. Tento proces může být velice zjednodušeně definován jako spisová služba.

Postupem času se systém spisové služby stále více zdokonaloval, ale také byrokraticky narůstal. Často byl nepružný, zdlouhavý a komplikovaný. Všechny informace byly po staletí uchovávány v listinné podobě. Nyní se situace mění. Využívají se jiná média pro záznam či uchovávání dokumentů. Přechod do etapy elektronizace a digitalizace je markantní a všudypřítomný. Jedná se o období, které se ve zpracování informací, resp. dokumentů obsahujících informace, radikálně mění. Ve vztahu ke spisové službě je možno hovořit o turbulentním období. Spisová služba se nachází na počátku své nové etapy. Jedná se o fázi, kdy se nastavují pravidla, podmínky a procesy jak pro práci s dokumenty, tak s jejich nakládáním a uchováváním. Po staletí byl systém práce s dokumenty převážně stejný. Jako médium pro uchování informací byl využíván papír, resp. listina. V 21. století nastává odklon od listinného dokumentu, vše se přesouvá do elektronického světa. S tím se ale snoubí řada nových výzev i pro spisovou službu. Právem se díky tomu očekává zeštíhlení a zjednodušení byrokratického aparátu, což ale zároveň na celý systém klade velké nároky a požadavky. Velká část požadavků směřuje do oblasti digitálních technologií, tedy vývoje odpovídajících aplikací v rámci podnikové architektury informačních systémů.

První kapitola, teoretická část diplomové práce, se bude zabývat českým i evropským právním rámcem elektronických systémů spisové služby. Seznámí s historií a vývojem spisové služby, pravidly a požadavky, které jsou na ni v elektronickém světě kladeny, a to jak v České republice, tak v rámci Evropské unie. Představí stěžejní právní předpisy ovlivňující chod elektronických systémů spisové služby a rovněž přiblíží životní cyklus dokumentu.

Druhá kapitola, praktická část, se bude zaměřovat na realizaci nových legislativních požadavků, které vstoupily v průběhu minulého roku v platnost. Zhodnotí dopad vybraných požadavků nejen na spisovou službu jako proces, ale především na vývoj SW aplikace či aplikací, ve kterých je spisová služba provozována. Práce se tak bude zaměřovat zejména na

nový legislativní požadavek, kterým jsou atestace elektronických systémů spisové služby veřejnoprávních původců.

Výsledkem práce bude syntéza získaných poznatků z právního stavu k 31. říjnu 2023, potvrzení či vyvrácení hypotéz z dílčích cílů a navržení alternativního řešení k současnému stavu informačních systémů spisové služby s cílem zlepšení kvality a zjednodušení tohoto procesu. S ohledem na aktuálně probíhající živou diskusi ve veřejnoprávním prostoru na téma elektronických spisových služeb budou uvedeny vlastní názory autorky jako možný příspěvek do této diskuse.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je analyzovat současný stav informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby a navrhnout alternativní řešení odlišná od současného stavu. Dílčím cílem je identifikace částí Národního standardu pro elektronické systémy spisové služby, které jsou z pohledu orgánů veřejné moci nadbytečné.

Na základě získaných informací a autorčiných praktických zkušeností budou formulovány návrhy především na racionalizaci postupů a zjednodušení výkonu veřejnoprávní agendy spisové služby.

2.2 Metodika

Teoretická část práce se zaměřuje na rešerši zákonů a odborné literatury ve státní správě, resp. u orgánů veřejné moci. Vychází z analýzy právních předpisů, odborné literatury a elektronických zdrojů vymezujících spisovou službu u veřejnoprávních původců. Následně popisuje a hodnotí současný stav a právní rámec u orgánů veřejné moci.

Praktická část, tzn. vlastní práce, je zaměřena na analýzu současného stavu informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby jako páteřního systému, a to včetně analýzy novelizací tří nejdůležitějších právních předpisů pro elektronické systémy spisové služby, kterými jsou zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů a Národní standard pro elektronické systémy spisové služby.

3 Teoretická východiska

3.1 Spisová služba

3.1.1 Definice spisové služby

Definice spisové služby předkládané v odborné literatuře jsou obdobné. Ve Slovníčku spisové služby a archivnictví (Skala, Vít, 2005, s. 57) je spisová služba popisována jako odborná správa dokumentů, které došly, anebo vznikly z činnosti původce nebo jeho právního předchůdce. Tato správa zahrnuje životní cyklus dokumentu, kterým je příjem, evidence, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání ukládání dokumentu a rovněž vyřazování dokumentu ve skartačním řízení. Součástí tohoto definování spisové služby je také kontrola výše uvedených činností.

Dobře nastavená spisová služba je důležitým pilířem každé organizace a její smysluplné a účelné vedení zajišťuje fungující chod dané organizace. Pokud je elektronický systém spisové služby (dále „eSSL“) funkční, kvalitní a důvěryhodný, spisová služba se dozajista stává páteřním systémem instituce. Velikost vnitřní organizační struktury společnosti a rozsáhlost jejích činností se zákonitě propisuje do složitosti systému spisové služby. Na eSSL mohou být následně navázány další samostatné evidence dokumentů, a to v souladu s vyhláškou č. 259/2012 Sb. § 8 odst. 2, kde je umožněna evidence stanovená jiným právním předpisem či spisovým řádem veřejnoprávního původce. Samostatná evidence dokumentů je pak samostatnou evidenční pomůckou, tzn. takové dokumenty následně nejsou evidovány v elektronickém systému spisové služby.

3.1.2 Cíle spisové služby

Cílem spisové služby je v první řadě zajištění správného průběhu životního cyklu dokumentu, a to včetně všech činností, které jsou se správou dokumentů spojené. Celý tento proces je legislativně ukotven, má své náležitosti a povinné atributy. Informační systém spisové služby má z pohledu celkové architektury organizace a případných řízených podřízených organizací pevně danou pozici a rovněž také odpovědnost. V prvé řadě se jedná o vedení jednotné evidence spisové služby, nezměnitelnost údajů, čistotu a nezávadnost dat, ale také efektivitu a přehlednost uživatelského prostředí. Rozměrnost elektronického systému spisové služby je odvislá od množství agend vykonávaných danou organizací, v našem případě orgánem veřejné moci. Na systém spisové služby jsou navázány agendové aplikace, které mají rovněž významný vliv na robustnost dané spisové služby.

3.1.3 Stručná historie spisové služby v českých zemích

Spisová služba není výdobytkem současné moderní doby, spisová služba prošla dlouhodobým historickým vývojem. V latině se setkáváme s pojmem „acta“, což značí plurál od českého slova „spis“, od kterého se odvíjí název spisová služba. Termín „ad acta“ označovaný zkratkou a/a se prolíná celou historií spisové služby a v administrativě je používán dodnes.

Kunt a Lechner (2017, s. 16) datují existenci moderní spisové služby přibližně od 16. století, kdy je používán pojem spis či akta pro označení souboru dokumentů. V této době vznikaly první postupy pro úřadování. Mezi významné panovníky, které je třeba s tvorbou spisové služby zmínit, patří Marie Terezie a Josef II. Císařovna Marie Terezie roku 1746 nařídila vést podací protokoly pro doručené dokumenty. Další významný krok učinil císař Josef II. roku 1781, kdy zavedl systém evidence využívající číslo jednací a podací protokol. Zavedení čísla jednacího zaručovalo, že každý rok se začalo počítat od jedničky, evidence tak byla snazší a přehlednější. Podací protokoly sloužily ke kontrole vyřízení všech došlých podání. Do tohoto období spadá i vytváření spisů pomocí tzv. priorace, která se týkala sloučení podání ve stejné věci, či bylo-li podnětem k dalšímu šetření, spojila se příslušná čísla jednací a byla evidována pod vyšším číslem jednacím.

Prioraci rovněž zmiňuje Sulitková (2017, s. 66) a to spolu se zavedením nových registraturních a kancelářských pomůcek, jako např. rejstříky neboli indexy, které sloužily k většímu zpřehlednění systému (např. abecední seznam hesel), či elenchy – archy sloužící k vyplňování při podání, později popisovaly obsah spisů vzniklých priorací. Velký rozvoj nastal v 18. století, kdy se formovaly principy spisové služby a začaly se používat v celém státním aparátu, nevyjímaje církev i tehdejší panství.

K další významnější změně spisové služby došlo dle Sulitkové (2017, s. 68-69) v druhé polovině 19. století, které je spojené s množstvím změn ve společnosti (průmyslová revoluce, občanská práva, rozšiřování veřejné správy atd.) a narůstáním byrokratického aparátu. Roku 1853 byl vydán jednací řád soudní a roku 1855 politický, narůstá množství dokumentů a dochází ke zvýšení administrativy a následně ke snahám o zefektivnění spisové služby. Vychází příručky o úřadování obecní a městské správy (např. z roku 1851 od Ferdinanda Stamma), ale na spisovou službu má víc než cokoli jiného vliv „osvícení reprezentanti“. Dochází ke změně ve vedení čísla jednacího a spisu. Ke spisu jsou přidávána další podání v téže záležitosti, a dochází k tomu, že spis je ukládán pod prvním číslem jednacím.

Sulitková (2017, s. 70) uvádí jako další významný krok zavedení spisovenské značky ve 30. letech 20. století. Pod spisovenskou značkou byl spis ukládán ve spisovně. Dnes je tato značka nazývána spisovým znakem.

Významným počinem bylo vydání prvního obecně závazného předpisu o vyřazování dokumentů. V roce 1951 byla ustanovena skartační subkomise Státní archivní komise, kterou byl vypracován návrh vyhlášky Ministerstva vnitra č. 62/1953 o zásadách pro vyřazování (skartaci) písemností. Jedná se o první obecně závazný právní předpis o vyřazování dokumentů státních orgánů, komunálních podniků i právnických osob (Štouračová, 1999, s. 114). Ač se jedná o vpravdě revoluční novinku, která výrazně změnila skartování dokumentů, jednalo se o předpis, který upravoval pouze část spisové služby, nikoli spisovou službu jako celek. V předpisu se zavádí povinnost vytvářet skartační návrhy a jsou dány na výběr tři skartační znaky „S“, „V“ a „A“ dle cennosti dokumentárního významu (Kunt, Lechner, 2017, s. 19, 132-133):

- Skartačním znakem „S“ (skart) jsou označeny písemnosti a spisy určené k likvidaci, tzn. písemnosti s nízkým dokumentárním významem.
- Skartačním znakem „A“ (archiválie) jsou označeny písemnosti a spisy určené k trvalé archivaci (uložení v archivu), tzn. písemnosti dokumentárně cenné.
- Skartační znak „V“ (výběr) umožňuje dodatečné posouzení písemnosti či spisu.

Uživatel se až následně rozhodnul, jak bude s dokumentem naloženo, tzn. změní-li se na skartační znak „S“ nebo „A“. (Kunt, Lechner, 2017, s. 19). Ačkoliv byl poslední novelizací zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále jen „ZASS“) skartační znak „V“ zrušen, bude jeho vypořádání přetrvávat s ohledem na dobíhající skartační řízení takto dříve označených dokumentů.

Prvním předpisem upravujícím oblast archivnictví bylo vládní nařízení č. 29/1954 Sb., o archivnictví, které bylo účinné od 9. června 1954. Gestorem archivnictví je jmenováno Ministerstvo vnitra. Poradním orgánem ve věcech vědeckých a archivně-odborných se stala vědecká archivní rada. Nařízení stanovilo postupy při skartačním řízení, a také povinnost vytvoření jednotného státního archivního fondu.

V roce 1974 byl vydán zákon č. 97/1974 Sb., o archivnictví (dále jen „ZOA“), který měl nahradit vyhlášku z roku 1954. Bohužel ani v tomto zákoně se zásadněji neřeší spisová služba (Kunt, Lechner, 2017, s. 20-21). Zákon č. 97/1974 Sb. v § 6 odst. 1 nově nařizoval, že: *„státní orgány a socialistické organizace zajišťují odbornou správu písemností, které vznikly z jejich činnosti, popřípadě z činností jejich předchůdců (včetně písemností došlých),*

a dbají o řádnou spisovou evidenci, o účelné a bezpečné uložení písemností a o jejich řádné vyřazování ve skartačním řízení“. Z tohoto zákona vyplývá, že oproti vyhlášce z roku 1953, byl kladen větší důraz na vyřazování dokumentů.

Nedostatky právních úprav spisové agendy se plně projevily po roce 1989. Rozsáhlé změny ve společnosti po konci komunistického režimu ukázaly, že tehdejší legislativa nebyla dostatečná. Zaniká československá federace, ruší se některé státní organizace a orgány, probíhá reorganizace státní správy a rozbíhá se privatizace. Jednalo se o velice dynamickou dobu, která s sebou přinesla mnoho nového, na což bylo třeba patřičně a zavčasu reagovat. Předpokládalo se, že nedostatky budou odstraněny přijetím novelizace ZOA (zákon č. 343/1992 Sb.), která například vymezila povinné subjekty. Nově jimi byly státní orgány a obce, následně jiné právnické osoby, včetně fyzických osob provozujících podnikatelskou činnost (Kunt, Lechner, 2017, s. 22).

ZOA byl ještě několikrát novelizován. Byla zde zřetelná snaha reflektovat všechny geopolitické změny té doby. Je třeba si uvědomit, že v období mezi lety 1989 a rokem 2000 docházelo k velkým společenským i politickým změnám. Tyto změny se týkaly nejen Československa, resp. České republiky, ale i celé Evropy. Existovala silná potřeba zbavit se byrokratického státu, dělat věci lépe, rychleji a efektivněji. Jednalo se o období, kdy se ve veřejném životě začíná objevovat elektronizace. Počítače se postupně stávají součástí pracovních procesů. Zprvu jen nahrazují psací stroje, ale dalo by se směle říct, že právě tento okamžik je prvním krokem k blížící se elektronizaci veřejné správy jako celku. V oblasti spisové služby byl vývoj završen přijetím bez nadsázky revoluční legislativní změny v ZASS. Než ale bude podrobně toto téma rozebráno, je třeba poukázat na mezinárodní kontext problematiky, kde stěžejním tématem je elektronická identita subjektu.

3.2 Evropský rámec elektronické identifikace

3.2.1 Nařízení eIDAS

Současné řešení elektronizace spisové služby v ČR nelze pochopit bez mezinárodního kontextu, kde klíčovou oblastí je problematika důvěryhodnosti a identifikace subjektů. V aplikacích elektronických spisových služeb představuje správné nastavení elektronických podpisů a elektronických pečetí jeden ze stěžejních ukazatelů kvalitní správy digitálních dokumentů. Jedná se o rozsáhlé téma, proto bude rozebráno podrobněji.

V rámci Evropské unie je velká snaha o vybudování důvěryhodnosti on-line prostředí a pocitu dostatku právní jistoty pro všechny občany Evropské unie. Mít občanskou

a právní jistotu v on-line světě je velice důležité a pro budoucí fungování rovněž nezbytné. Dokázat se dostatečně identifikovat i v digitálním světě a přijmout tento druh komunikace za obvyklý není úplně snadné. Jsme na prahu doby, kdy elektronická komunikace jasně udává směr. E-mailová a elektronická komunikace napříč Evropou se stává zcela standardní. Platí to ovšem i ve vztahu on-line komunikace mezi orgánem veřejné moci jedné členské země a občanem jiné členské země Evropské unie? Velice zjednodušeně by se dalo říct, že tomu brání pouze naše vnitřní bloky a hranice, protože systém identifikace a verifikace v on-line prostředí je nastaven a právně ošetřen. Občan se tudíž musí „pouze“ zřetelně a jednoznačně identifikovat nejenom např. svým občanským průkazem fyzicky, ale rovněž svou nezaměnitelnou a jedinečnou identitou v on-line světě.

Jednotná pravidla nastavuje nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, známého také pod zkráceným názvem „nařízení eIDAS“. Nařízení bylo vydáno v Úředním věstníku Evropské unie (L 257/73) dne 28. srpna 2014 s cílem vybudovat důvěryhodnost v on-line prostředí, které má markantní význam pro hospodářský a sociální rozvoj. Snaží se eliminovat nedostatek právní jistoty, který mohou občané Evropské unie v on-line prostředí pociťovat. Usiluje o podnícení důvěryhodnosti v elektronické transakce na vnitřním trhu poskytnutím společného základu pro bezpečnou elektronickou komunikaci mezi všemi subjekty veřejného života, kterými jsou občané, podniky a orgány veřejné moci. Směrnice Evropského parlamentu a Rady (EU) 1999/93/ES se věnovala elektronickým podpisům, nebrala ovšem ještě zřetel na přeshraniční a meziodvětvový rámec pro bezpečné, důvěryhodné a lehce použitelné elektronické transakce.

3.2.2 Služby vytvářející důvěru

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, je platný a účinný od 19. září 2016. Tento zákon specifikuje postupy kvalifikovaných poskytovatelů služeb vytvářejících důvěru, řeší problematiku podepisování a pečetění dokumentu a poskytování služeb vytvářejících důvěru Správou základních registrů.

Nařízením eIDAS je stanovena povinnost každého členského státu Evropské unie vytvářet, udržovat a zveřejňovat důvěryhodné seznamy, kde jsou zaznamenány informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru, a to včetně informací

o poskytovaných kvalifikovaných službách vytvářejících důvěru, kterou jednotliví poskytovatelé nabízejí.

3.2.3 Elektronická identifikace

Donát, Maisner a Piffl (2017, s. 45) upozorňují na to, že díky nařízení eIDAS a s tím spojenou elektronickou identifikací vzniká nová, do té doby právně nedefinovaná, zóna. Nejprve je nutné definovat pojem „elektronická identifikace“, „systém elektronické identifikace“ a „autentizace“. Elektronickou identifikací je míněno označení pro postup používání osobních identifikačních údajů v elektronické podobě, díky kterým je jedinečně identifikována daná osoba, ať už fyzická či právnická. Systémem elektronické identifikace je pak takový systém elektronické identifikace, na jehož základě jsou právě výše uvedeným osobám vydávány prostředky pro elektronickou identifikaci. Autentizace je vysvětlována jako postup, při kterém je umožněno potvrzení elektronické identifikace osoby nebo původ a integrita dat v elektronické podobě. Je možné doplnit, že prostředky pro elektronickou identifikaci jsou hmotné (např. USB token) a nehmotné (např. certifikát v počítači) a obsahují osobní identifikační údaje používané k autentizaci.

Elektronická identita slouží k identifikaci konkrétní osoby v rámci jednání v online prostředí. V reálném životě se běžně využívá identifikace osob (např. nahlášení jména a data narození u lékaře) i jejich autentizace prostřednictvím ověření totožnosti dané osoby. Prostředkem pro identifikaci je následně např. občanský průkaz nebo cestovní pas.

Nařízení eIDAS v článku 8 stanovuje tři základní úrovně záruky neboli důvěry identifikačních prostředků, a to nízkou, značnou a vysokou úroveň.

- Nízká úroveň záruky umožňuje pouze omezenou míru spolehlivosti ověření identity. Převážně se jedná o tzv. jednofaktorovou autentizaci. Příkladem nízké úrovně záruky je zadání ID jména a hesla, např. při vstupu do datové schránky.
- Zaručená úroveň záruky umožňuje vyšší úroveň ověření. Jedná se o dvoufaktorovou autentizaci. Je zde použito uživatelské jméno a heslo (viz nízká úroveň) a zároveň dochází k ověření totožnosti ještě dalším způsobem, např. zasláním SMS kódu.
- Vysoká úroveň záruky umožňuje nejvyšší úroveň ověření. Účelem je předejít zneužití nebo změně totožnosti, proto je při ověření identity používán ještě fyzický identifikační prostředek (např. token nebo kontaktní čip), kde je třeba pro

přihlášení ještě zadat přístupové údaje (Donát, Maisner, Piffl, 2017, s. 65). Příkladem vysoké úrovně záruky je občanský průkaz s čipem, kde se zadává PIN.

Nařízení eIDAS se mimo jiné zaměřuje na rozpoznání elektronické identity (dále „eIdentita“) z jiných členských států, a jejich verifikaci napříč Evropskou Unií. eIdentita je prostředek pro identifikaci a autentizaci občanů on-line služeb veřejné správy. Tento prostředek elektronické komunikace je garantován státem a zakotven v legislativě České republiky.

Od 18. srpna 2017 je platný zákon č. 250/2017 Sb., o elektronické identifikaci, jehož účinnost je od 1. července 2018. Zákon o elektronické identifikaci představuje právní základ pro prokazování totožnosti s využitím elektronické identifikace. Elektronická identifikace, která je brána jako důvěrná, musí být provedena prostřednictvím tzv. kvalifikovaného systému elektronické identifikace.

Na základě zákona o elektronické identifikaci vytvořilo Ministerstvo vnitra České republiky státní informační systém Národní bod pro identifikaci a autentizaci (dále „NIA“), který garantuje zprostředkování důvěryhodné elektronické identifikace vůči základním registrům. Poskytovatelé eIdentity musí mít přístup k zaručeným informacím o osobách, kterým eIdentitu poskytují. Mezi takové informace patří například jméno, příjmení, datum narození, adresa trvalého bydliště (Jarolímek a kol., 2021, s. 40-41).

Stát, resp. Ministerstvo vnitra ČR, jako garant této služby nabízí v České republice následující identifikační prostředky, kterými jsou:

- občanský průkaz s aktivovaným elektronickým čipem (elektronický čip musí být aktivovaný po 1. červenci 2018);
- NIA ID (identifikační prostředek založený na kombinaci jména, hesla a SMS kódu);
- mobilní klíč eGovernmentu (přihlašování bez následných ověřovacích kódů).

Službu elektronické identifikace poskytují jak státní orgány, tak soukromé subjekty, jimž Ministerstvo vnitra České republiky uděluje akreditaci pro správu kvalifikovaného systému elektronické identifikace. Zákon těmto kvalifikovaným správcům systémů elektronické identifikace stanovuje základní povinnosti nutné pro správný výkon jejich činnosti, tzn. pro správu kvalifikovaného systému elektronické identifikace.

Na českém trhu jsou nabízeny služby soukromoprávních kvalifikovaných poskytovatelů, kterými jsou:

- bankovní domy (ČSOB Identita od Československé obchodní banky a. s., Bankovní Identita od České spořitelny a. s., Bankovní identita KB od Komerční banky a. s., aj.);
- První certifikační autorita a. s. s čipovou kartou Starcos;
- zájmové sdružení právnických osob CZ.NIC s projektem MojeID.

S poskytováním eIdentity je úzce spojena bezpečnost dané služby. eIDAS sjednotilo používání elektronických autentizačních prostředků, zavedlo kvalifikované elektronické autentizační prvky zajišťující důvěryhodnost elektronických dokumentů, mezi které patří kvalifikovaný elektronický podpis, kvalifikovaná elektronická pečeť a kvalifikované časové razítko. eIDAS rovněž poskytuje seznam důvěryhodných služeb a zabývá se zaručenými a uznávanými elektronickými podpisy. Právě elektronický podpis je při identifikace tím stěžejním institutem pro použití elektronických dokumentů, a to jak z hlediska jejich autenticity, tak jejich právní validity (Kunt, Lechner, 2017, s. 60).

Dalším bodem, kterému se nařízení věnuje, je specifikace požadavků na elektronickou identifikaci. Jednotlivé unijní státy musí implementovat do svých systémů prostředky pro elektronickou identifikaci osob.

V České republice byl 24. srpna 2016 vydán zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v kterém byly zapracovány požadavky eIDAS. Zákon ustanovuje Ministerstvo vnitra ČR dohlížitelem a garantem v této oblasti. V zákoně jsou jasně definované postupy kvalifikovaných poskytovatelů služeb vytvářejících důvěru.

Kvalifikovaná elektronická pečeť

Kvalifikovaná elektronická pečeť nahradila dřívější elektronickou značku (zákon o podpisu). Kvalifikovaná elektronická pečeť může být využita pouze právnickými osobami s cílem zaručit jejich pravost a neměnnost. Slouží jako důkaz toho, že dokument vydala určitá právnická osoba. Poskytuje tak jistotu o jeho původu. Není proto určen jednotlivým fyzickým osobám, ale výhradně organizacím, jako jsou např. orgány veřejné moci. Nejedná se o automatizovanou funkcionalitu, dokument je pečetěn cíleně tím, kým je vytvářen. Dalším specifikem je, že nevyjadřuje vůli. Rovněž pro ni platí domněnka integrity dat a správnosti původu. Kvalifikovaná pečeť se užívá tehdy, kdy právní předpis nestanovuje povinnost použít elektronický podpis. Kvalifikovaná elektronická pečeť je povinně

uznávaná v rámci celé Evropské unie, na rozdíl od dalších třech typů pečetí, kterými je pečeť prostá, zaručená a zaručená s certifikátem (Kunt, Lechner, 2017, s. 62) a eIDAS.

Kvalifikované časové razítko

Kvalifikované časové razítko jsou data v elektronické podobě spojující další data rovněž v elektronické podobě (např. dokument), a to v určitém časovém okamžiku. Kvalifikované časové razítko umožňuje prokázat čas jeho vytvoření. Prokazuje, že dokument v té době a podobě již existoval. Elektronický podpis prokazuje pouze identitu autora dokumentu, resp. osoby, která dokument po jeho vytvoření podepsala. Neobsahuje však v sobě žádnou průkaznou informaci, kdy byl dokument vytvořen, resp. podepsán. Elektronický podpis obsahuje pouze čas vytvoření podpisu převzatý z média (počítače, telefonu aj.), na kterém byl podpis vytvořen, a proto není dostatečně průkazný. Namísto toho čas v kvalifikovaném časovém razítku je koordinovaný světovým časem. Je tak prodloužena ověřitelnost elektronického podpisu. Časové razítko je připojováno spisovou službou orgánu veřejné moci ke každému podepsanému či zapečetěnému elektronickému dokumentu a to vždy, jedná-li takovým dokumentem stát nebo orgán veřejné moci. Rovněž je možné ověřit, zda byl dokument od okamžiku přiložení časového razítka změněn (Kunt, Lechner, 2017, s. 63-65).

Elektronické podpisy

Hlavním smyslem elektronického podpisu je ověření identity občana v elektronickém světě. Prokazuje se tak, že občan, který elektronický podpis použil, je opravdu tou osobou, za kterou se vydává. Rovněž je možno zkontrolovat, zda byl dokument po připojení elektronického podpisu změněn či nikoli (Jarolímek a kol., 2021, s. 46). V praktickém životě je taková verifikace nespornou výhodou a platnost podpisu je uznávána v rámci celé Evropské unie.

Zpočátku používání elektronických podpisů byl elektronický podpis definován jako údaj v elektronické podobě. Existuje však vícero způsobů elektronického podpisu. Mezi některé patří sken vlastnoručního podpisu, sken razítka a připojení vlastnoručního podpisu dané osoby, heslo, PIN kód atd. Připojený elektronický podpis k datové zprávě určoval totožnost osoby, která dokument podepsala (Donát, Maisner, Piffl, 2017, s. 31).

Důležitost elektronického podpisu je enormní, proto se elektronickým podpisům eIDAS věnuje. Je třeba si uvědomit, že elektronický podpis má nezaměnitelnou a

nezpochybnitelnou funkci. Legislativně byl v České republice institut elektronického podpisu ošetřen zákonem č. 227/2000 Sb., o elektronickém podpisu, než byl nahrazen právě nařízením eIDAS a následně také zákonem č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Zákon č. 298/2016 Sb. nabyl platnosti i účinnosti dne 19. září 2016.

U elektronického podpisu se předpokládají a vyžadují vlastnosti jako je autenticita, integrita, nepopiratelnost a časový rámec. Autenticita elektronického dokumentu zaručuje, že dokument pochází od ověřeného uživatele. Integrita zaručuje nezměněnost a neporušenost daného dokumentu, což znamená, že do dokumentu nebylo následně zasahováno a nebyl měněn. Nepopiratelností je míněno to, že podpis na dokumentu nemůže jeho autor popřít. Je prokazatelně uvedeno, která osoba je autorem daného dokumentu. Časový rámec potvrdí čas prokazatelné existence dokumentu v dané podobě (Jarolímek a kol., 2021, s. 63).

Jarolímek a kol. (2021, s. 47) vidí nespornou výhodu elektronického podpisu právě v jeho univerzálnosti během elektronické komunikace a povinnosti jeho uznávání i v zahraničí. Každý elektronický podpis je unikátní a jedinečný. Elektronický podpis neovlivňuje ani software, ani hardware. Pokud si tedy uživatel dostatečně chrání podpis před krádeží nebo jiným zneužitím, jedná se o vysoce využitelný prostředek. Pokud v běžném životě člověk ztratí osobní doklad, jeho ztrátu může zjistit hned a k zablokování ztraceného či odcizeného průkazu může dojít prakticky okamžitě. Při zneužití podpisu tomu tak ale být nemusí.

Brom (2013, s. 31) definuje tři základní funkce elektronického podpisu:

- elektronický podpis označuje osobu, která dokument podepsala (tzn. činila úkon);
- osoba, která dokument podepsala, ho podepsat v té dané konkrétní podobě také chtěla;
- je možno ověřit totožnost takové osoby.

Nařízením eIDAS jsou definovány čtyři úrovně elektronického podpisu, kterými jsou:

- elektronický podpis;
- zaručený elektronický podpis;

- zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis;
- kvalifikovaný elektronický podpis.

Kvalifikovaný elektronický podpis

Kvalifikovaným elektronickým podpisem se dle článku 3 odst. 12 nařízení eIDAS rozumí: „*zaručený elektronický podpis, který je vytvářen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy*“. Kunt a Lechner (2017, s. 61) zdůrazňují, že pouze tento druh podpisu je dán na úroveň podpisu vlastnoručního.

Podepisování

Podepisování dokumentu se věnuje § 5 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, kde je jasně stanoveno, že k podepisování elektronickým podpisem je možno použít pouze kvalifikovaný elektronický podpis, podepisuje-li se jím dokument, kterým je právě jednáno, a to ze strany orgánu veřejné moci atd. či osoby při výkonu své působnosti. Dalším paragrafem je doplněno, že k podepisování elektronickým podpisem je možno použít pouze uznávaný elektronický podpis, kterým se právě jedná vůči veřejnoprávnímu podepisujícímu. Uznávaným elektronickým podpisem je zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. Z výše uvedeného je patrné, že v úředním styku je nezbytně nutné používat uznávaný elektronický podpis. Ze strany orgánu veřejné moci je povoleno užití pouze kvalifikovaného elektronického podpisu. Kvalifikovaný elektronický podpis je roven podpisu vlastnoručnímu.

Pomocí kvalifikovaného certifikátu je možno vytvořit zaručený elektronický podpis, který je uznáván všemi orgány veřejné moci v České republice. Pokud je využit pro vygenerování klíčů a uložení certifikátů kvalifikovaný prostředek, získá občan možnost vytvářet kvalifikované elektronické podpisy, což je nejvyšší forma elektronického podpisu povinně uznávaná i v celé Evropské Unii.

Kvalifikované certifikáty jsou využitelné například při komunikaci s úřady (Finanční správa České republiky, Celní správa České republiky, Česká správa sociálního zabezpečení, soudy aj.) a zdravotními pojišťovnami, dále při odesílání datových zpráv, pokud má společnost více jednatelů, při využívání elektronických formulářů a e-podatelny, při

archivaci dokumentů nebo při práci s e-tržišti (elektronické tržiště). Jedná se o malý výčet činností, při kterých jsou kvalifikované certifikáty využitelné.

Komponentou podpisu je certifikát. Certifikátů je celá řada a jsou různé úrovně. V občanském životě je možno se setkat s certifikáty vydanými zaměstnavatelem, bankovním domem, internetovými servery apod. Certifikáty pro široké využití jsou vydávány obecně uznávanými autoritami. Rozlišujeme kvalifikovaný a komerční certifikát. Kvalifikovaný certifikát, nutný pro styk v rámci veřejné a státní správy, vydávají v České republice obecně uznávané autority, kterými je Česká pošta, s. p. (Post Signum), eIdentity a. s (eIdentity) a První certifikační autorita, a. s. (I. CA) (Jarolímek a kol., 2021, s. 66). Nově je tato dosavadní trojice poskytovatelů rozšířena o Národní certifikační autoritu (Národní CA), která v roce 2019 přibyla na Sezam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovatelů kvalifikovaných služeb vytvářejících důvěru.

Jedná se o dva soukromé subjekty (eIdentity a. s., První certifikační autorita a. s.), státní podnik Česká pošta, a s. a Správu základních registrů, který splnil požadavky Ministerstva vnitra ČR a byl nově zařazen mezi obecně uznávané autority.

3.2.4 Elektronický dokument

V eIDAS dochází k definování termínu „elektronický dokument“, jímž je míněn jakýkoli obsah, který je uchován v elektronické podobě. Do této kategorie spadá text a nahrávka zvuková, vizuální a audiovizuální. Elektronický dokument se stává základní jednotkou elektronické komunikace, a to jak v rámci jednotlivých států, tak v rámci přeshraniční komunikace, transakcí a spolupráce. Elektronický dokument může být opatřen kvalifikovaným elektronickým podpisem, kvalifikovaným elektronickým časovým razítkem nebo kvalifikovanou elektronickou pečetí.

Rozdíly mezi jednotlivými typy zajištění jsou následující:

- Je-li elektronický dokument opatřen kvalifikovaným elektronickým podpisem, je mu uděleno stejné právní postavení jako listině podepsané vlastnoručním podpisem.
- Je-li opatřen kvalifikovaným elektronickým časovým razítkem, panuje domněnka správnosti data a času, v kterém byl dokument vytvořen, s čímž je spojena i integrita dokumentu.
- Pokud je opatřen kvalifikovanou elektronickou pečetí, zůstává domněnka integrity dat v elektronickém dokumentu a potvrzuje se rovněž správnost původu dokumentu (Donát, Maisner, Piffl, 2017, s. 166-167).

Na nařízení eIDAS reagovala Česká republika přijetím zákona č. 298/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Zákon nabyl účinnosti dne 19. září 2016. Zákon stanovuje pro veřejnoprávní původce povinnost opatřit právně jednající dokumenty kvalifikovanými autentizačními prvky. Právním jednáním je míněno chování osoby, jež vyvolává právní následky, které jsou z takového jednání zřejmé a vyplývají buď ze zákona, dobrých mravů, zvyklostí nebo ze zavedené praxe stran. K právnímu jednání je zapotřebí projevená vůle navenek s právními následky. V případě, kdy orgán veřejné moci v danou chvíli nejedná, může být k autentizaci použit zaručený elektronický podpis, uznávaný elektronický podpis nebo kvalifikovaná elektronická pečeť (Kment, 2018, s. 66).

Problematika spojená s elektronickou identitou, jejím prokazováním a důvěryhodností, a dále problematika elektronických dokumentů je pouze částí elektronizace veřejné správy, pro kterou se vžil pojem eGovernment. Jednotlivé procesy, které eGovernment zahrnuje, se bytostně dotýkají elektronizace spisové služby, proto je nutný podrobnější výklad tohoto pojmu.

3.3 Vývoj eGovernmentu

Na eGovernment je možno v moderní společnosti pohlížet jako na elektronizaci veřejné správy s použitím digitálních, informačních a komunikačních technologií. Jedná se o elektronickou interakci mezi veřejnou správou a občanem. Tato interakce má být ve svém důsledku rychlá, dostupná, spolehlivá a samozřejmě že i po stránce finanční výrazně levnější. Štědroň (2007, s. 12) definuje eGovernment jako sérii procesů, které umožňují výkon veřejné správy, zároveň se zde ale uplatňují práva a povinnosti jak fyzických, tak právnických osob, a to za realizace elektronických prostředků, kdy služba veřejné správy je poskytována široké veřejnosti, a přitom je rychlá, spolehlivá a levná. Jak uvádí Špaček (2012, s. 3), veřejná správa je tu pro veřejnost a má jí sloužit, k čemuž je třeba využívat informačních a komunikačních technologií (tzv. ICT) na takové bázi, aby byly zajištěny a podpořeny poskytované služby veřejnosti, a to i v případech, kdy veřejná správa ve svých aktivitách spíše nabývá vrchnostenských podob (např. vyžaduje či až vynucuje procedury předepsané legislativou).

3.3.1 eGovernment v České republice

Jednou z důležitých oblastí eGovernmentu je elektronizace spisové služby. Spisová služba se stále vyvíjí, hledají se nové směry a objevují se nové trendy. Konec 20. století

s sebou přinesl rozvoj v informačních a elektronických technologiích, což se rovněž promítlo do spisové služby a došlo k masivní změně v celém jejím pojetí. Spisová služba už není pouze nástrojem evidence dokumentů, ale stává se součástí informačního systému dané organizace. Digitalizace a elektronizace systém spisové služby posouvá rychle kupředu a je velkým mezníkem v jejím vývoji. Je zřejmé, že některé postupy ve spisové službě přetrvávají staletí, jsou stále aplikovatelné a jejich použití je vhodné i v současné době. Principy nastolené v 50. letech minulého století daly základní rámec současné české spisové službě a vchází z nich i spisová služba nynější (Kunt, Lechner, 2017, s. 22).

Digitalizace a elektronizace spisové služby je dalším nutným krokem v jejím vývoji. Současná doba je milníkem ve způsobu komunikace. Ustupuje psaní dopisů a podávání písemných žádostí prostřednictvím klasických poštovních služeb. Nastupuje doba, kdy je vše možno vyřídit on-line. Informace, zprávy, sdělení – vše je možno vyřídit takříkajíc hned, a to z počítače, tabletu, telefonu. Je otázkou okamžiku poslat zprávu blízké osobě, ale také podat žádost na úřad, vyřídit jednoduché požadavky, zaplatit účty. Občané právem vyžadují, aby stejným způsobem mohli komunikovat např. s orgány veřejné moci.

3.3.2 Počátky eGovernmentu v České republice

Počátky eGovernmentu v České republice sahají do roku 1999. V tomto roce vchází v platnost zákon č. 106/1999 Sb., o svobodném přístupu k informacím, s účinností od 1. ledna 2000. Od tohoto roku je možné podávat žádosti o informace, a to prostřednictvím elektronické pošty. V roce 2000 dochází k zavedení institutu elektronického podpisu do českého právního řádu díky zákonu č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Dalo by se očekávat, že bude v krátkém sledu následovat prováděcí protokol elektronického podpisu, ale ten byl aplikován až po roce a půl od jeho zavedení.

První kroky eGovernmentu jsou spjaté s dokumentem Státní Informační politika – cesta k informační společnosti, který byl považován za první koncepci informační politiky a byl přijat v České republice. Koncepce budování informačních systémů veřejné správy (dále „ISVS“) z roku 1999 navazovala právě na tento dokument. Koncepce se prolínala mezi jednotlivými vládními ministerstvy, změny měly být řešeny formou projektového meziresortního řešení úkolů. Oporou pro reorganizaci se měl stát právě zákon o ISVS. Koncepce se mimo jiné věnovala také registrům a kladla si za cíl vytvoření komplexního systému popisujícího procesy, vazby a metainformační systémy datového obsahu ISVS.

Koncepce rovněž zmiňovala jako jeden ze svých hlavních bodů zavedení základních registrů, kde by se soustředila veškerá sebraná data napříč orgány veřejné moci v celé České republice. Nahradily by se tak registry v tom čase běžné, které schraňovaly a uchovávaly jen omezený objem informací, často se opakovaly a dublovaly. Jednalo se do jisté míry o privátní registry daných orgánů veřejné moci. Jednotlivé registry spolu nekomunikovaly, informace nesdílely a v důsledku toho bylo běžné, že občané neustále vyplňovali stejné informace při kontaktu s daným orgánem veřejné moci, potažmo úředníkem. Základní registry by naopak byly na jednom místě, dostupné pro všechny orgány veřejné moci a informace v nich by byly celistvé, úplné a přesné (Špaček, 2012, s. 55).

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, vešel v platnost 23. října 2000. Jeho cílem byla větší efektivita a bezpečnost komunikace ve veřejné správě. Právě tímto zákonem byla zajištěna ochrana a bezpečnost v rámci provozovaných informačních systémů, byla nastavena povinnost atestací z hlediska standardů informačních systémů a rovněž byl definován požadavek na uplatnění standardu ve všech fázích životního cyklu informačních systémů. Garantem eGovernmentu se stal Úřad pro veřejné informační systémy, který byl vytvořen právě zmíněným zákonem. Jeho prioritními úkoly bylo vytváření ISVS a jejich rozvoj. Měl analyzovat potřeby ISVS. Mimo jiné tento úřad vydával pověření k výkonu atestací ISVS fyzickým či právnickým osobám (Špaček, 2012, s. 55). I přes velké plány a vize měl Úřad pro veřejné informační systémy slabé postavení a v roce 2003 se přetransformoval v Ministerstvo informatiky České republiky. Další nově vzniklou institucí byl Úřad pro ochranu osobních údajů. Ministerstvo informatiky ČR plnilo dle „autora“ spíš roli propagační a reprezentativní, než aby zaštiťovalo vývoj a rozvoj eGovernmentu ve všech státních institucích. Ministerstvo informatiky ČR ale bylo k 1. červnu 2007 zrušeno a kompetence přešly na Ministerstvo vnitra České republiky. Od 1. dubna 2023 jsou tyto kompetence v gesci Digitální a informační agentury (dále jen „DIA“). DIA začala svoji činnost 1. dubna 2023. Jejím cílem je zajišťování digitalizace veřejné správy České republiky, ale také posílení a sjednocení digitální transformace veřejné správy a zlepšení poskytovaných služeb občanům. Činností DIA je rovněž zlepšení digitální úrovně České republiky v rámci Evropské unie, se kterou na určitých programech spolupracuje (např. digitální identita).

3.3.3 eGovernment současné doby

Ministerstvo vnitra jako současný hlavní garant eGovernmentu uvádí, že hlavní ideou eGovernmentu je správa věcí veřejných, a to právě s použitím současných moderních elektronických nástrojů. Díky těmto nástrojům se předpokládá, že veřejná správa jako celek bude k občanům přátelštější a zároveň jako služba dostupnější, efektivnější, rychlejší a v neposlední řadě rovněž levnější.

Do portfolia eGovernmentu lze zařadit následující projekty: základní registry, Czech POINT, datové schránky, portál veřejné správy, portál občana, komunikační infrastrukturu veřejné správy a centrální místo služeb KIVS/CMS a také ISVS (informační systém veřejné správy – Obchodní rejstřík, Živnostenský rejstřík, Rejstřík trestů atd.). U vybraných pilířů eGovernmentu, které nejvíce souvisí s problematikou výkonu spisové služby, následuje podrobnější popis.

Czech POINT

Czech POINT je ošetřen zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, platný od 23. října 2000 a účinný od téhož data, tj. 23. října 2000. Czech POINT je zkratka znamenající Český podací ověřovací a informační národní terminál a je asistovaným místem výkonu veřejné správy, kde občané mohou získat širokou paletu informací o jejich osobě, majetku a právech, jako je např. ověřený výpis z Rejstříku trestů a ze základních registrů, matriční informace, bodové hodnocení řidiče, ověřené výpisy z Katastru nemovitostí nebo Obchodního rejstříku, autorizovaná konverze aj. Dle Lechnera (20113, s. 196) je právě Czech POINT nejúspěšnějším projektem eGovernmentu. S tímto názorem nezbývá než souhlasit. Opravdu se jedná o vlajkovou loď celého eGovernmentu, o službu, která je mezi obyvateli nejznámější a nejvyhledávanější.

Autorizovaná konverze je zakotvena v zákonu č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Autorizovanou konverzi provádí kontaktní místa veřejné správy (Czech POINT, notáři, obecní úřady, pobočky České pošty, s. p. aj.), advokáti a orgány veřejné moci. Je možno rozlišit dva druhy autorizované konverze, a to autorizovanou konverzi na žádost a autorizovanou konverzi z moci úřední. Autorizovaná konverze na žádost je prováděna na kontaktních místech Czech POINT a je zpoplatněna jednotnou sazbou za každou započatou konvertovanou stranu, jedná se o správní poplatek. Obecně platí, že orgány veřejné moci si mohou konvertovat dokumenty pro výkon své

působnosti, a právě v tomto případě se jedná o autorizovanou konverzi z moci úřední. Právní účinky konvertovaných dokumentů jsou shodné jak pro konvertování na žádost, tak z moci úřední. Autorizovaná konverze znamená úplné převedení dokumentu v listinné podobě do podoby elektronické, anebo naopak, tzn. úplné převedení dokumentu v elektronické podobě do podoby listinné. Součástí konverze je také ověřovací doložka. Ověřovací doložka je připojena na konec konvertovaného dokumentu a obsahuje potvrzující údaje o subjektu (název orgánu veřejné moci, jméno odpovědného pracovníka), který konverzi provedl, pořadové číslo konverze, údaje o počtu listů, datu a čase vzniku konverze (Brom, 2013, s. 67-68).

Datové schránky

Informační systém datových schránek je upraven zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů. Zákon je platný od 19. srpna 2008 a účinný od 1. července 2009. Datové schránky jsou elektronickým úložištěm a primárně slouží ke komunikaci s orgány veřejné moci. Každá datová schránka má svůj vlastní jedinečný a nezměnitelný identifikátor, což je zaručeno § 21 výše uvedeného zákona. Zřizovatelem informačního systému datových schránek (dále „ISDS“) je Ministerstvo vnitra České republiky, které je rovněž spravuje. Provozovatelem ISDS je Česká pošta, s. p., držitel poštovní licence v České republice. Ač by se mohlo na první pohled jevit, že je tato služba zdarma, protože se vše děje on-line prostředí, není tomu tak. Datové zprávy zasílané mezi orgány veřejné moci navzájem a mezi orgány veřejné moci a právnickou či fyzickou osobou mající zřízenou datovou schránku jsou hrazeny ze státního rozpočtu. Zpoplatněno je odesílání datových zpráv mezi soukromými subjekty (tzn. vyjma orgánů veřejné moci). Prostřednictvím datových schránek jsou doručovány datové zprávy. Datové schránky mají nespornou výhodu v rychlosti a prokazatelnosti doručení datových zpráv. Doručením datových zpráv, resp. dokumentu, je brán okamžik přihlášení pověřené osoby do příslušné datové schránky. Při doručování datovou schránkou lze též využít zákonného institutu doručení fikcí. Proti výpočtu doby doručení se ovšem staví rozsudek Nejvyššího správního soudu (čj. 4 Afs 264/2018-85) ze dne 26. května 2022, který se vyjádřil k otázce aplikace pravidel počítání času ve vztahu k doručování do datové schránky a zohlednil aplikování pravidla o posouvání konce lhůty na nejblíže následující pracovní den. Tzn., že datové zprávy doručené v sobotu, neděli nebo o svátek jsou nově brány jako doručené první následující pracovní den. V návaznosti na tento rozsudek byly správcem ISDS, resp.

Ministerstvem vnitra České republiky, upraveny doručenky datových schránek. Existuje několik druhů datových schránek, a to jak zřízených na základě zákonné povinnosti, tak zřízených výhradně na žádost. Mezi subjekty s povinnou datovou schránkou patří orgány veřejné moci, osoby fyzické, podnikající fyzické a právnické, které jsou v roli orgánu veřejné moci, právnické osoby zapsané v obchodním rejstříku, podnikající fyzické osoby-advokáti, daňoví poradci, insolvenční správci, statutární auditoři, znalci, soudní překladatelé nebo tlumočníci. Nově mají povinnost mít datovou schránku rovněž podnikající fyzické osoby (např. živnostník), tudíž všem těmto subjektům byly datové schránky k 1. lednu 2023 zřízeny.

Základní registry

Základním registrům se věnuje zákon č. 111/2009 Sb., o základních registrech, který je platný od 27. dubna 2009 a účinný od 1. července 2010. Základní registry patří mezi hlavní body eGovernmentu a jsou funkční od roku 2012. Poskytují aktuálně platné informace, tzn. bez historie, a jsou přístupné jen oprávněným osobám. Rozeznáváme čtyři základní druhy registrů:

- ROS – Registr osob, který sdružuje aktuální informace o právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci (subjekt je identifikován jednoznačným identifikátorem, kterým je identifikační číslo). ROS využívají všechny orgány veřejné správy, které k tomu mají oprávnění z Registru práv a povinností. Správcem je Český statistický úřad.
- ROB – Registr obyvatel, který sdružuje referenční údaje o osobách žijících a evidovaných na území České republiky. Mezi takové osoby patří státní občané České republiky a cizinci pobývající na území ČR mající trvalý pobyt, dlouhodobé vízum nebo povolení k dlouhodobému pobytu, azyl či občané členských států Evropské unie v rámci trvalého pobytu či pobytu delšího než 3 měsíce. Správcem je Ministerstvo vnitra ČR.
- RPP – Registr práv a povinností, který slouží jako zdroj údajů pro informační systémy základních registrů, sumarizuje jednotlivé agendy a poskytuje údaje o nich. Rovněž eviduje údaje o oprávněných osobách majících k těmto agendám přístup a osobám majícím přístup k údajům v ostatních registrech. Správcem je Ministerstvo vnitra ČR.

- RÚIAN – Registr územní identifikace, adres a nemovitostí, který eviduje údaje o územních prvcích, územně evidenčních jednotkách, adresách, územní identifikaci a údajů o účelových územních prvcích. Správcem je Český úřad zeměměřický a katastrální.

3.4 Elektronická spisová služba

3.4.1 Spisová služba v legislativě České republiky

V roce 2004 byla přijata nová revoluční právní úprava archivnictví a spisové služby. ZASS nabyl účinnosti 1. ledna 2005. Jedná se o významný milník v historii spisové služby, protože je to poprvé, kdy je zákonem upravována celá oblast archivnictví a spisové služby.

ZASS je klíčovým právním předpisem pro tuto práci. Komplexně vymezuje principy spisové služby – upravuje problematiku dokumentu a jeho životního cyklu, nakládání s dokumenty v celé jejich šíři a rovněž výběr a evidenci archiválií včetně jejich ochrany a následné badatelské činnosti. Dále stanovuje soustavu archivů a vymezuje působnost Ministerstva vnitra České republiky a dalších správních orgánů.

Kunt a Lechner (2022, s. 29-32) poukazují na to, že ZASS byl od svého vzniku v roce 2004, resp. od nabytí účinnosti v 1. ledna 2005, novelizován již 23krát. Novelizace se týkaly zejména rychle se rozvíjející elektronizace ve veřejné správě a procesů s tím spojených, a dále přijímání dalších zákonů propisujících se do správného chodu spisové služby. Původní znění zákonu například neuvádělo povinnost vést spisovou službu v elektronické podobě. V zákoně bylo pouze uvedeno, že původce vykonává písemnou nebo elektronickou formu spisové služby za pomoci výpočetní techniky.

ZASS není jediný právní akt, kterým je spisová služba legislativně vymezena, regulována a ošetřena. Kunt a Lechner (2017, s. 23) poukazují na to, že ve vztahu ke spisové službě je třeba zahrnout všechny procesní právní předpisy, mezi které patří vedle správního a daňového řádu rovněž občanský soudní řád, soudní řád správní a trestní řád.

Ve vývoji legislativy, která se dotýká spisových služeb, lze identifikovat několik etap:

První etapa

První etapu je možno datovat od 1. ledna 2005, kdy vešel v účinnost ZASS, až do 30. června 2009 v souvislosti s účinností zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Do této etapy spadá první prováděcí vyhláška, kterou byla vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby, s účinností od 1. ledna 2005. Stanovila se zde možnost za určitých podmínek vést spisovou službu v elektronické podobě (Brom, 2013, s. 26). Dále stanovila povinnost elektronických dokumentů se skartačními znaky „A“ a „V“, u nichž není možné uložení ve formátu zaručujícím jejich neměnnost včetně následného budoucího čtení, aby byly nejpozději před zařazením do skartačního řízení vytištěny a následně opatřeny náležitostmi originálu v době vyřízení dokumentu. Dokumenty v analogové formě rovněž se skartačními znaky „A“ a „V“ měly být vytištěny na trvanlivém papíru, a to z důvodu případné degradace dokumentu způsobeného kyselostí papíru běžného (Kunt. Lechner, 2022, s. 32).

První prováděcí vyhláška č. 646/2004 Sb. byla ještě v průběhu první etapy nahrazena vyhláškou č. 191/2009 Sb., o podrobnostech výkonu spisové služby, platná od 26. června 2009 a účinná od 1. července 2009.

Dalším legislativním aktem, který by v této etapě neměl být opomenut, je novela archivního zákona, tj. zákon 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. Platnost tohoto zákona je od 26. června 2009 a účinnost od 1. července 2009. Zákon č. 190/2009 Sb. upřednostnil elektronicky vedenou spisovou službu se všemi náležitostmi s tím, že určení původci měli na implementaci elektronické spisové služby do svých systémů lhůtu do 30. června 2012 (Brom, 2013, s. 26).

Posledním legislativním aktem zmíněným v této etapě je pak publikace prvního Národního standardu pro elektronické systémy spisové služby (dále „NSESSL“). Jedná se o velice důležitý předpis, který se stává nedílnou součástí při implementaci elektronických systémů spisové služby u veřejnoprávních původců. Vzhledem k jeho důležitosti v rámci elektronizace systémů spisových služeb je třeba se s ním blíže seznámit.

Národní standard pro elektronické systémy spisové služby zveřejňuje Ministerstvo vnitra České republiky na základě § 70 odst. 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění zákona č. 190/2009 Sb. a zákona č. 167/2012 Sb. Ministerstvo vnitra zveřejní aktuální platnou verzi národního standardu ve věstníku a na webových stránkách ministerstva. První verze NSESSL byla zveřejněna ve Věstníku Ministerstva vnitra v roce 2009 (publikováno v VMV čá. 76/2009).

První verze NSESSL obsahovala 12 kapitol a celkem 773 požadavků. Požadavky se dělily na povinné a doporučené. Ovšem rozdělení požadavků se ukázalo jako vcelku

nesnadné a už v roce 2010 došlo k úpravě, kdy některé požadavky byly ze skupiny povinných přesunuty mezi nepovinné.

NSESSL navazuje rovněž na MoReq 2010, který byl představen na setkání DLM Forum a AGM konaném v Budapešti v roce 2011. MoReq 2010 nespecifikuje konkrétní řešení, ale zavádí a definuje základní prvky, které by měl obsahovat systém spisové služby v práci s dokumenty. Vzhledem k tomu, že je MoReq 2010 modulárním systémem, je možno ho přizpůsobit dle rozličných požadavků různých původců.

Druhá etapa

Druhou etapu je možno datovat od účinnosti zákona č. 300/2008 Sb. dne 1. července 2009 do 31. července 2012 v souvislosti s účinností nové prováděcí vyhlášky ZASS (vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby).

Po turbulentní první etapě nastává relativně klidnější druhá etapa, kdy byly uvedeny v život datové schránky, a tudíž i tolik očekávaná elektronická komunikace právě jejich prostřednictvím, a v které vstupuje v platnost druhá verze NSESSL, zveřejněného ve Věstníku Ministerstva vnitra v roce 2010 (publikováno v VMV čá. 101/2010).

Důležitými vyhláškami, které bezprostředně navazují na zákon č. 300/2008 Sb., je vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů a vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Třetí etapa

Třetí etapu zahrnuje období od 1. srpna 2012 do 2. července 2017, v souvislosti s účinností čtvrté verze NSESSL.

Třetí etapa je etapou plné elektronizace. Tato etapa je primárně spojena s vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby, která vstoupila v platnost 26. července 2012, s účinností od 1. srpna 2012. Tato vyhláška je pro spisovou službu a její vedení hned po ZASS nejdůležitějším právním aktem. Vyhláška je souhrnným právním předpisem, který se podrobně věnuje výkonu spisové služby u veřejnoprávních původců. Vyhláška reflektuje změny v ZASS i eIDAS. Samozřejmě že i ona dostála několika změnám, a to díky nutnosti reflektovat na změny ostatních zákonů. Nakonec se vyhláška ustálila na celkem 29. paragrafech, které popisují životní cyklus dokumentů v organizaci – příjem, evidenci (tvorbu čísla jednacího i evidenci dokumentů v samostatných evidencích

dokumentů, tvorbu spisů atd.), oběh, rozdělování, vyhotovování dokumentů, podepisování a vyřizování, ukládání a vyřazování dokumentů.

Třetí verze NSESSL byla zveřejněna ve Věstníku Ministerstva vnitra v roce 2012 (publikováno v VMV čá. 64/2012). V NSESSL se nejednalo o změny zásadní. Došlo např. k úpravě chybných schémat, a to hlavně u schémat entit, následně byla změněna a doplněna schémata XML.

Čtvrtá etapa

Čtvrtá etapa je období od 3. července 2017 (účinnost čtvrté verze NSESSL) do 31. ledna 2022 (novelizace ZASS, kterou byly zavedeny povinné atestace elektronických spisových služeb).

Důvodem pro vydání dalšího nového NSESSL (publikován ve Věstníku Ministerstva vnitra – VMV čá. 57/2017) byla dle Kunta a Lechnera (2022, s. 48) komplikovaná struktura NSESSL, neodpovídající postup výkonu spisové služby dle vyhlášky č. 259/2012 Sb. a odlišnost od spisového plánu mezi touto vyhláškou a NSESSL, problémy s transakčním protokolem a potřebu standardizace vazeb mezi eSSL a dalšími systémy, které vytvářejí dokumenty u daného původce. Tento NSESSL prošel značnou změnou, při čemž např. došlo k vypuštění všech doporučených požadavků, které dosud byly součástí každé verze NSESSL.

Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, tzv. zákon DEPO

Čtvrtou etapu ukončil DEPO, který je významným milníkem v provádění eGovernmentu v ČR. Zákon byl platný od 9. července 2021 a účinný od 1. února 2022. Tímto zákonem se změnilo přes 160 právních předpisů souvisejících s další elektronizací postupů orgánů veřejné moci – mimo jiné ZASS. Zákon DEPO se snaží svými změnami prohloubit elektronizaci veřejné správy a prohloubit eGovernment v České republice, čímž by se měla rovněž výrazně zjednodušit elektronická komunikace mezi občany a úřady. DEPO například značně rozšiřuje používání datových schránek, resp. rozšiřuje okruh osob, které budou mít ze zákona zřízenou datovou schránku, a tudíž které budou s úřady jednat elektronicky. Datovou schránku získá automaticky také každý občan, který se ke službám státu přihlásí svou elektronickou identitou, např. do Portálu občana.

DEPO dále podporuje vylepšení stávající právní úpravy využívání cloud computingu (internetového úložiště) orgány veřejné správy. Očekává se od toho intenzivnější využívání cloud computingu při vytváření a provozu informačních systémů veřejné správy. Následné budování i provoz ISVS by měl být díky tomu levnější.

Dalším významným bodem v DEPO je zjednodušení systému určování údajů využívaných jednotlivými úřady z ISVS. Díky registru práv a povinností pak bude možné snadno zjistit, k jakým údajům má úřad přístup. Rovněž tak občané a právnické subjekty nebudou muset dokládat své údaje při komunikaci s úřadem. Nebude nutné pro ně hlásit změny ani ve vztahu k poskytovatelům komerčních služeb (telefonní provider, bankovní domy aj.). Tyto informace i pro poskytování v rámci komerčních služeb bude ze stejné úrovně zabezpečení údajů jako v případě orgánů veřejné moci.

Významným bodem v DEPO je pak pro eSSL zavedení povinného atestování elektronických systémů spisové služby. Měl se tím vytvořit předpoklad pro kvalitnější výkon spisové služby orgány veřejné moci. Existoval předpoklad, že atestace eSSL, povinnost vykonávat výlučně elektronickou spisovou službu urychlí a zefektivní zpracovávání podání fyzických a právnických osob a zrovna tak vnitřní provoz orgánů veřejné moci.

Pátá etapa

Pátá etapa započala 1.února 2022, a to v souvislosti s povinností atestovat elektronické spisové služby. V návaznosti na DEPO proběhly legislativní úpravy, a to s účinností k 1. únoru 2022 ZASS a dále k 1. červenci 2023, kdy vstoupila v platnost novelizace vyhlášky č. 259/2012 Sb. a rovněž NSESSL, jehož nová verze byla publikována 30. června 2023 ve Věstníku Ministerstva vnitra České republiky (publikováno ve Věstníku MV čá. 42/2023). Tato etapa stále trvá.

Dne 1. července 2023 vstoupila v platnost vyhláška č. 96/2023 Sb., kterou se mění vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů. Novelizace se týká všech částí životního cyklu dokumentu. Některé změny jsou formální drobnosti, ale jiné jsou opravdu zásadní (např. povinnost vkládat dokument do spisu). Takové změny se nevyhnou transformaci v obsahu práce a pracovních činnostech uživatelů jednotlivých eSSL. Zavedení těchto změn do praxe klade požadavky na metodiky spisové služby jednotlivých organizací.

Jako druhý se o narovnání snaží NSESSL. Na NSESSL je pohlíženo částečně jako na technický dokument, který popisuje fungování eSSL právě v souladu s ZASS a vyhláškou

č. 259/2012 Sb. Je to právě NSESSL, podle kterého pracovníci spisové služby, informatici a vývojáři postupují za účelem implementace bodů NSESSL do jednotlivých elektronických spisových služeb. NSESSL proto musí mít jasnou oporu v ZASS a ve vyhlášce č. 259/2012 a musí s nimi korespondovat.

3.4.2 Základní pojmy

Elektronizací spisové služby se do jazyka SSL implementuje a redefinuje nová terminologie. Nejmarkantnější změnou je opuštění pojmu písemnost, který je nahrazen pojmem dokument. Mezi nově používané pojmy, které se staly součástí běžného názvosloví spisové služby, je možno zařadit pojem komponenta, číslo jednací, jednoznačný identifikátor, metadata, transakční protokol, spis, výstupní formát atd. Výše uvedené termíny jsou vysvětleny v následujícím textu.

Dokument

Dokument je základní jednotkou spisové služby. Díky významné elektronizaci celého procesu spisové služby došlo v posledních letech k nahrazení původního termínu písemnost právě termínem dokument. Lechner (2020, s. 15) upozorňuje na fenomén, že termín „listina“ a „písemnost“ jsou příbuznými pojmy k „dokumentu“ a ač jsou sice v běžné praxi termíny listina a písemnost vztahovány převážně k listinám papírovým, jedná se o mylný názor. Listina i písemnost mohou být ve formě elektronické i listinné. Následně odkazy na odbornou literaturu a příklady ze soudní praxe poukazuje na to, že výše uvedené pojmy jsou si významem příbuzné a nelze je striktně oddělit.

Používaný pojem „dokument“ představuje do jisté míry neutrální termín, ale zároveň širší ve svém významu, což také potvrzuje ZASS, v němž je dokument definován jako: *„každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové, či digitální, která byla vytvořena původcem nebo byla původci doručena*“. Kunt a Lechner (2017, s. 73) poukazují na definici dokumentu, kterou uvádí evropská norma MoReq2, podle které jsou dokumenty vytvořené, přijaté a uchovávané informace mající důkazní hodnotu nebo vycházejí-li z právních závazků či obchodních vztahů. V novější verzi MoReq2010 je přisouzena dokumentu ještě větší důležitost tím, že je definován jako informace mající vnitřní hodnotu, která ho dělá natolik důležitým, že je třeba ho uložit a bezpečně uchovat (Lechner, 2013, s. 77). Pod neutrálním názvem dokument může být více formátů zprávy, nejen písemná podoba textu. Může jít o zvukovou nebo obrazovou zprávu

či záznam např. na nosiči CD/DVD/flash disku nebo jiném médiu. Dokumentem může být film, kniha, dopis, vzkaz.

Komponenta

V nové verzi NSESSL došlo ke změně v obsahu pojmu komponenta. Dříve se dokument sestával z komponent, které tak tvořily jeho součást. Komponenta měla podobu digitální nebo analogovou. Příkladem komponent byl průvodní dopis a příloha. V analogové podobě byla komponenta dále nedělitelná. V digitální podobě se na komponentu hledělo jako na jednoznačně vymezený proud bitů tvořící počítačový soubor. V nové verzi NSESSL je ovšem komponentou nazýván: „*jednoznačně vymezený proud bitů tvořící datový soubor charakterizovaný zpravidla formátem datového souboru, běžně zpracovávaným programovými aplikacemi, které umožňují provádět správu souborů, složek a disků tak, aby k nim bylo možné uživatelsky srozumitelně přistupovat a s nimi samostatně manipulovat*“. To znamená, že komponenta má pouze digitální podobu, a tudíž toto označení se týká výhradně elektronického dokumentu a nikoli analogového.

Metadata

Dlouhodobě jsou metadata vykládána jako data, jejichž smyslem je popis souvislostí, obsahu, struktury a správy daného dokumentu v průběhu času. Metadata dokumentu jsou strukturovaná data, která poskytují informace o primárních datech na elektronických a digitalizovaných dokumentech. Existuje více typů metadat. Pro spisovou a archivní službu jsou primárně využívána metadata administrativní. Do administrativních metadat je možno zařadit metadata archivační, právní a technická. V takovém případě metadata zaznamenávají informace o tom, kdo a kdy dokument či soubor vytvořil a jak bylo s dokumentem dále nakládáno, o počtu stran, skartačním znaku, o typu souboru (jakou má soubor příponu) atd. Zkráceně je možno říct, že metadata zaznamenávají data o datech.

Spis

Lechner (2020, s. 15-16) definuje spis jako soubor dokumentů či zaznamenaných informací. Rovněž poukazuje na to, že ačkoli je dokumentu v ZASS věnována značná část co do podrobnosti popisu jeho funkcionalit, u spisu to tak není. Je zde řešen pouze v rovině obecné, která se týká jeho životního cyklu, tzn. založení, vyřízení, uzavření a uložení. Spis by se dal přitom charakterizovat jako základní evidenční jednotka, jež popisuje a sdružuje ve své celistvosti dané řízení, anebo řešení jedné určité věci. Spisů následně může být tolik

druhů, kolik je různých procesních specifik. Lechner rozlišuje spis soudní, trestní, správní, insolvenční atd.

Zákon č. 500/2004 Sb., správní řád, účinný od 1. ledna 2006, formuluje spis a jeho náležitosti. Spis tvoří převážně podání, protokoly, záznamy, rozhodnutí atd. Do spisu jsou zahrnuty důkazní prostředky, kterými mohou být záznamy zvukové, obrazové či záznamy na elektronických nosičích. Spisu, a to hlavně jeho tvorbě a práci se spisy, se věnuje rovněž ZASS a vyhláška č. 259/2012 Sb. v § 12.

Tvorba a způsob vedení spisu musí být ukotven ve spisovém řádu dané organizace, kde jsou pevně a jasně specifikovány požadavky na vedení a tvorbu spisu. Spis v elektronické podobě má obsahovat určité pevně dané informace, jako je např. jednoznačný identifikátor spisu a spisová značka, datum založení a uzavření spisu, spisový znak a skartační režim spisu, stručný obsah spisu atd.

Každý spis je označován spisovou značkou. Struktura spisové značky není přesně daná, je odvislá od různých druhů původců i různých typů řízení (Lechner, 2020, s. 26). Součástí spisu je rovněž jeho spisový přehled neboli soupis, kde jsou zaznamenány všechny jeho součásti, přílohy, data vložení do spisu či jejich vyjmutí. Do spisu pak mohou být vkládány v průběhu životního cyklu dokumentu další dokumenty související s danou věcí.

Dle Lechnera (2020, s. 25-27) může mít spis formu listinnou, elektronickou nebo hybridní, kdy jde o kombinaci prvních dvou variant. Hybridní spis obsahuje dokumenty jak v elektronické, tak v listinné podobě a již z jeho názvu je patrné, že se jedná o kombinaci obou typů spisu. S termínem hybridního spisu se v legislativě nepracuje, přesto se jedná o vhodné vyjádření obsahu spisu. Lechner (2020, s. 26) zde dále upozorňuje na stanovisko Národního archivu, který rozeznává pouze dva typy spisu, a to elektronický a analogový, přičemž analogovým spisem je rovněž spis elektronický obsahující i jen jedinou analogovou komponentu.

Třetí verze NSESSL zavádí nový pojem spisu, a to spis typový. Jsou tedy nově rozlišovány dva typy spisu, a to „spis“ a „typový spis“. Typový spis je soubor dokumentů s předem stanovenou strukturou. Dělí se na součásti, které se člení na díly. Součásti typového spisu jsou dle svého obsahu stanovené části a každá taková část se dělí na díly. Do dílů se zařazují dokumenty. Kunt a Lechner (2017, s. 82) dále upřesňuje, že základním odlišujícím znakem typových spisů je skutečnost, že typový spis je výsledkem jednotlivých opakujících se činností. Typové spisy jsou z toho důvodu často velmi obsažné. Používají se v rámci známého a předem stanoveného procesu. Typové spisy jsou proto často vedeny dlouhodobě,

často až desítky let. Typový spis se nevyřizuje jako běžný spis, a to z toho důvodu, že slouží k ukládání. Příkladem typového spisu může být spis daňový, který představuje daňovou agendu daného daňového subjektu. Do daňového spisu jsou ukládány všechny dokumenty týkající se daňových řízení a jiných činností, které s daňovými řízeními mohou souviset.

Jmenný rejstřík

Jmenný rejstřík jako nástroj reflektuje Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Zkráceně se o tomto nařízení hovoří jako o „obecném nařízení o ochraně osobních údajů“, ve zkratce GDPR. V české legislativě tuto oblast upravuje zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

ZASS uvádí, že ve jmenném rejstříku jsou vedeny údaje o odesílatelích a adresátech dokumentů. Jedná se tedy o adresné údaje, datum narození, příp. rodné číslo či údaje odlišující fyzickou osobu od právnické či nepodnikající osoby. Jmenný rejstřík dle ZASS slouží k automatické práci s údaji o odesilateli či adresátovi dokumentu, které jsou evidované v eSSL. Jmenným rejstříkem se zabývá rovněž DEPO, tzn. zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci platný od 1. července 2022. Na jmenný rejstřík je pohlíženo jako na samostatnou funkční částí eSSL. Sdružuje zpracovávané informace osobních údajů. Díky tomu dochází k sloučení osobních údajů či údajů o právnických osobách v jednom centrálním místě eSSL, nejsou tak roztroušeny v popisných datech dokumentů. Jmenný rejstřík je možno nazvat základní centralizovanou evidenční pomůckou při zpracování osobních údajů v rámci dané eSSL. Tato evidenční pomůcka obsahuje povinně a nepovinně vedené údaje. Povinně vedené údaje jsou stanoveny § 64 odst. 5 zákona č. 499/2004 Sb. (např. jméno/jména a příjmení u fyzických osob, obchodní firmu/název u podnikajících fyzických osob zapsaných v obchodním rejstříku, identifikátor datové schránky, identifikační číslo osoby aj.). Nepovinně vedené údaje u fyzických osob jsou např. datum/místo narození, současná adresa aj. Je třeba zdůraznit, že jmenný rejstřík musí obsahovat takové penzum informací, aby byla fyzická osoba ztotožnitelná rovněž dle správního řádu (např. § 18 odst. 2 zákona č. 500/2004 Sb., správního řádu).

Pojem veřejnoprávní původce

Pro obsah této práce je nutné rovněž definovat a vymezit pojem veřejnoprávního původce. Tento pojem je uváděn v ZASS, kde má veřejnoprávní původce stanovené povinnosti, mezi něž patří například povinnost vykonávat spisovou službu, uchovávat dokumenty a následně umožnit výběr archiválií. Povinnost vykonávat spisovou službu je rozdělena do dvou skupin dle typu veřejnoprávního původce. Spisová služba je poté vykonávána buď v plném rozsahu (u veřejnoprávních původců) nebo v omezeném rozsahu (u určených původců).

Dle § 3 odst. 1 ZASS jsou veřejnoprávním původcem:

- organizační složky státu;
- ozbrojené síly a bezpečnostní sbory;
- státní příspěvkové organizace a státní podniky;
- územní samosprávné celky, jejich organizační složky či právnické osoby zřízené či založené územními samosprávnými celky;
- vysoké školy, školy a školská zařízení s výjimkou mateřských a výchovných škol;
- veřejné výzkumné instituce;
- právnické osoby zřízené zákonem;
- zdravotní pojišťovny.

Určenými původci jsou pak dle ZASS (§ 63 odst. 1) kraje a hlavní město Praha, obce s pověřeným obecním úřadem a obce se stavebním nebo matričním úřadem, městská část nebo městský obvod územně členěného statutárního města a městská část hlavního města Prahy.

3.4.3 Životní cyklus dokumentu

Životní cyklus dokumentu vzniká vytvořením dokumentu a je zakončen jeho skartací. Lechner (2013, s. 111-112) dělí životní cyklus elektronického dokumentu do čtyř etap, kterými jsou tvorba, využití, uchování a následná archivace. Následuje popis jednotlivých etap (Lechner, 2013, s. 111):

Tvorba dokumentu

Jedná se o období, kdy buď elektronický originál dokumentu přímo vzniká, nebo je vytvářen převodem z dokumentu analogového, tzn. z listinného dokumentu. K takovému převodu dochází při použití autorizované konverze.

Využití dokumentu

Dokument je veden, spravován a zpracováván v systému spisové služby dané organizace. V tomto období probíhají příslušná úřední řízení. Dokument může být veden samostatně nebo může být založen do spisu. Dokument je součástí vnitřního cyklu organizace, kdy je předáván na oddělení, přidělován, podepisován atd. Rovněž k němu mohou vznikat odpovědní dokumenty či může být postoupen k řešení na jiný správní orgán. Jedná se o období, kdy je s dokumentem aktivně pracováno a nakládáno. Tato životní etapa dokumentu by se dala nazvat tak, že dokument je v „akci".

Uchování dokumentu

Pokud je projednávaný případ vyřešen a uživatel se k jeho obsahu již nebude vracet, dokument je uzavřen. Dokument je následně uložen ve spisovně, a to fyzické nebo elektronické. Ve spisovně může být dokument uložen samostatně nebo je součástí uzavřeného a uloženého spisu. Životnost dokumentů a spisů uložených ve spisovně je řízena spisovým plánem dané organizace.

Jakkoliv je provozována spisová služba v elektronické podobě, žádný z veřejnoprávních původců se prozatím nevyhne nutnosti uchovávat také listinné dokumenty. Dokumenty a spisy v listinné podobě se ukládají do spisoven, případně do příručních registratur (jiný název „příruční spisovna"). Příruční registratura může být zřízena u jednotlivých uživatelů nebo na příslušných útvarech či odděleních dané organizace. Dokumenty a spisy jsou zde uloženy po nezbytně nutnou dobu, než jsou následně předány do spisovny. Spisovna je místo zřízené danou organizací, kde jsou fyzicky uloženy uzavřené a zpracované dokumenty a spisy do doby ukončení skartačního řízení.

Spisovna musí splňovat dané předpoklady, mezi které patří například:

- ochrana před světelnou škodlivostí, kdy okna mají být upravena tak, aby do místnosti neproniklo přímé sluneční záření;
- ochrana před plynným a prašným znečištěním;
- místnost archivu se nesmí nacházet v záplavových či jinak rizikových oblastech, jako je např. startovací a přistávací koridor letecké dopravy;
- blízko umístění spisů nesmí vést plynové a vodní potrubí, parovod, kanalizace dešťové vody a splašek, ani sítě a rozvodna elektrické energie;
- prostory musí být řádně odvětrávány pro zachování stálé teploty a vlhkosti;
- úložné prostory a vnitřní materiál spisovny musí být z nehořlavých materiálů;

- dokumenty s magnetickým záznamem musí být chráněny před účinky elektromagnetického pole;
- spisovna musí být vybavena elektrickou požární signalizací, včetně jejího systému, musí splňovat speciální požadavky.

Pro ukládání elektronických dokumentů a spisů je zřízena elektronická spisovna. Elektronická spisovna se zabývá uložením elektronických dokumentů a spisů dané organizace převážně ve střednědobém a dlouhodobém horizontu. Je definována legislativou a zároveň potřebami dané organizace. Systém elektronické spisovny musí umět pracovat s dokumenty, které vznikly v různých systémech a aplikacích, jako jsou například elektronická podatelna, elektronický systém spisové služby, agendové aplikace a další systémy. Během uložení dokumentu v elektronické spisovně musí být zaručeno, že se uzavřené dokumenty a spisy nesmí změnit. Pro jejich uchování je třeba se řídit předepsaným způsobem. V elektronické spisovně musí být dokumenty chráněny před ztrátou, zničením a změnou, musí být zaručena jejich důvěryhodnost, tzn. u uložených informací musí být zaručena nezměněnost a prokazatelnost vzniku v uvedeném čase. Další důležitou podmínkou je jejich čitelnost, a to i v budoucnosti. Důležité je si uvědomit, že některé dokumenty a spisy mají velmi dlouhou skartační dobu (např. personální spisy mají skartační dobu 40-50 let), a přesto musí být zachovány nezměněny po celou dobu uchování v elektronické spisovně, ale zároveň musí obsahovat všechny autentizační prvky a musí být i v budoucnu čitelné. Proto nesmí být opomenut také rychlý technologický vývoj. Digitalizace a elektronizace se rychle vyvíjí. Co bylo inovativní před několika lety, může být už v současnosti běžné či dokonce zastaralé, a ne zrovna bezpečné.

Jarolímek a kol. (2021, s. 62) řadí mezi největší hrozby v uchování dat degradaci nosiče, zastarávání hardware a software, zastarávání formátu a ztrátu platnosti autentizačních prvků. Další velkou diskutovanou kapitolou je zajištění bezpečí dokumentů a spisů. Je třeba si uvědomit, že ztráta dokumentů dokladujících vnitřní procesy dané organizace (např. orgánu veřejné moci), či jejich důvěryhodnost, může představovat obecné riziko, které může souviset s právní jistotou, jednoznačností i vymahatelností.

Archivace dokumentu

Jedná se o poslední fázi životního cyklu dokumentu. Po uplynutí skartační lhůty je dokument a spis zařazen do skartačního řízení. Skartační řízení je postup, při kterém se vyřazují dokumenty, kterým uplynula skartační lhůta a které jsou nadále nepotřebné pro

činnost původce. Skartační řízení je prováděno na základě skartačního návrhu. Během skartačního řízení dochází k výběru dokumentů, které se vyřazují nebo jsou navrhovány za archiválie. Dokumenty a spisy jsou označeny skartačními znaky „A“ (archiválie) a „S“ (skart) dle své důležitosti a cennosti dokumentárního významu. Skartační znak „V“ (výběr) už se v aktuální legislativě neobjevuje. Po uplynutí skartační lhůty dojde k posouzení, zda se skartační znak „V“ změní na skartační znak „S“ nebo „A“, a nadále je ve skartačním řízení veden pod novým skartačním znakem. Dokument je označen skartačním znakem, spis je jako celek označen skartačním znakem, který odpovídá dokumentu s nejvyšší hodnotou skartačního znaku v daném spisu (S < V < A, resp. S < A).

Skartační návrh uvádí celkový rozsah dokumentů navržených ke skartaci, charakterizuje jejich obsah, uvádí dataci (tzn. období) a také skartační režim.

Součástí skartačního režimu je skartační znak, skartační lhůta a spouštěcí událost. Na stanovení skartační lhůty mají vliv různé faktory, a patří ke složitým činnostem původce dokumentu. Je třeba zohlednit požadavky jiných právních předpisů (např. obecná promlčecí lhůta), obecně však je nucen stanovit ji na základě možného využití dokumentu pro budoucí vlastní činnost. Přitom je nutné postupovat s ohledem na veřejný zájem. Částečná změna ve výpočtu skartační lhůty nastala vydáním Nařízení Evropského parlamentu a Rady (EU) 2016/679 dne 27. dubna 2019 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – tzv. GDPR). Tímto je uděleno právo subjektu údajů požádat o informace ve věci zpracovávání osobních údajů, jež se ho týkají. De facto jde o to, že je třeba respektovat právo na sdělení, jak dlouho budou dokumenty obsahující osobní údaje uloženy u původce/organizace (tedy skartační lhůta), a na zdůvodnění, jakým způsobem a z jakého titulu (na základě jakých právních norem) byla tato doba stanovena. Původce dokumentu tak musí být připraven vysvětlit stanovenou délku skartační lhůty, resp. vysvětlit, z jakého titulu si dokument ponechal tak dlouho. Zatímco skartační znak („S“, „V“, „A“) vyjadřuje hodnotu dokumentu podle jeho obsahu a je rozhodující pro posuzování dokumentu ve skartačním řízení, skartační lhůta stanovuje dobu, po kterou musí dokument být uložen ze správních, právních či zákonných důvodů ve spisovně. Vyjadřuje se počtem roků, formou celého kladného čísla a poznamenává se za skartačním znakem (příklad: S3 – skartační znak S, skartační lhůta 3 roky). Původce je povinen se při skartaci a při vytváření skartačního návrhu řídit vnitřním předpisem organizace, kterým je Spisový a skartační řád.

Spisový a skartační řád poskytuje závazné postupy při výkonu spisové služby v podmínkách dané organizace. Je zpracován v souladu s příslušnými nařízeními, zákony a vyhláškami na úseku archivnictví a spisové služby. Strukturu spisového a skartačního plánu tvoří hierarchicky uspořádané věcné skupiny, do kterých se zatřiďují dokumenty. Zatříděním pod spisový znak je určena „životnost“ dokumentu v dané organizaci.

Archivace je prováděna buď veřejnými nebo soukromými archivy. Archiv je instituce, která všestranně pečuje o archiválie, stará se o jejich bezpečné uložení, odborně je zpracovává. Archivní síť v České republice tvoří archivy veřejné a archivy soukromé.

Archivace listinných dokumentů se zdá být snadná, a to z důvodu, že je léty vyzkoušená a prověřená. Lidé věky uchovávají, třídí a schraňují rozličné druhy písemností a dokumentů. Archivace analogových dokumentů má proto svou dlouholetou historii a tradici, během které došlo k vysledování a zavedení těch nejlepších způsobů a postupů v jejich archivaci.

Archivace se týká samozřejmě také elektronických dokumentů. Oproti archivaci analogových dokumentů se jedná o relativně nový druh archivace, který se ovšem dostal do popředí zájmu díky preferované elektronizaci a digitalizaci veřejné správy a služeb poskytovaných občanovi. K tomu účelu je primárně pro orgány veřejné moci zřízen Národní digitální archiv (dále „NDA“), jehož cílem je zajištění uchování digitálních archiválií vybraných veřejnými archivy, a to v dlouhodobém horizontu a rovněž následné případné zpřístupňování dokumentů v digitální podobě. Vybudováním projektu NDA je naplňována strategie veřejné správy pod názvem Smart Administration – Efektivní veřejná správa a přátelské veřejné služby. V usnesení vlády č. 11 ze 7. ledna 2004 je stanovena potřeba řešit archivaci narůstajícího množství elektronických dokumentů, a to takovým způsobem, aby nedošlo k devalvaci jejich důvěryhodnosti a průkaznosti přenesením na jiné médium (nosič), protože dokumenty ověřené zaručeným elektronickým podpisem by přenesením na klasický nosič ztratily svoji průkaznost. Následně by musely být po převedení znovu podepsány klasickým podpisem, což je proti smyslu celé koncepce elektronizace dokumentů. Mezi hlavní cíle Národního digitálního archivu patří stanovit a specifikovat požadavky, jak nakládat s elektronickými dokumenty, aby se zachovala jejich důvěryhodnost, čitelnost a také dostupnost v dlouhodobém horizontu.

3.4.4 Životní cyklus dokumentu v rámci orgánu veřejné moci

Spisová služba představuje soubor činností spojený se zpracováním a správou dokumentů a zajišťuje jejich odbornou správu během celého životního cyklu dokumentu v dané organizaci. Součástí životního cyklu dokumentu v organizaci jsou tyto etapy: příjem, evidence a označování, rozdělování, vyřizování, odesílání, ukládání a vyřazování dokumentů (Sulitková, 2017, s. 88-95). Níže jsou jednotlivé etapy popsány.

Příjem dokumentů

Příjem dokumentu musí u veřejnoprávních původců být zajištěn na místě k tomu určeném, kterým je podatelna. Vyhláška 283/2014 Sb. uvádí, že podatelnou musí procházet všechny zásilky určené původci, ať již jsou doručovány poštou, osobně či jinak. Díky tomuto ustanovení je pamatováno i na dokumenty, které se do organizace mohou dostat jiným způsobem než podatelnou, např. e-mailovou komunikací. V takovém případě musí dojít ze strany zaměstnance organizace k doručení dokumentu v co nejkratší době na podatelnu, kde bude následně zaevidován. Podatelna zpravidla přijímá došlé dokumenty bez ohledu na způsob doručení, odesílatele nebo místo odeslání. Na požádání musí být přijetí podání přebírajícím zaměstnancem podatelny potvrzeno pomocí štítku, popř. otiskem podacího razítka, a podpisem přebírajícího zaměstnance. U datových zpráv a dokumentů v nich obsažených proběhne kontrola na přítomnost škodlivého kódu. Proces kontroly by měl být zajišťován v rámci bezpečnostního systému informačních služeb dané organizace.

Všechny analogové dokumenty doručené na podatelnu musí být pracovníky podatelny opatřeny štítkem, a to co nejdříve po doručení. Výjimečně mohou být opatřeny otiskem podacího razítka, kde ovšem musí být doplněny všechny náležitosti přijetí. V případě, že se obálka na podatelně neotvírá (např. doručení přihlášky do výběrového řízení), je štítkem či otiskem podacího razítka označena pouze doručená obálka.

Za doručený dokument v analogové podobě je považován také dokument, který je předán osobně zaměstnanci mimo podatelnu (např. při osobním jednání či řízení) nebo je zaměstnance vytvořen mimo organizaci (např. protokol o kontrole, protokol o šetření). V takovém případě musí zaměstnanec zajistit bezodkladné přijetí, označení a zaevidování dokumentu v organizaci.

Na podatelně je možno také přijmout označený nosič dat (flash disk, CD/DVD disketa apod.), který je přijat a zaevidován, jestliže je k němu přiložen průvodní dopis s informacemi o odesilateli, adresátovi a o obsahu daného nosiče dat.

V některých případech se může stát, že například dokument v analogové podobě není čitelný nebo je neúplný. V takovém případě nemusí být k zaevidování přijat a je odmítnut.

Dokument v digitální podobě se považuje za dodaný organizaci, je-li dostupný podatelně. Pokud ovšem elektronický dokument datové zprávy obsahuje škodlivý kód, tzn. neprošel antivirovou kontrolou, či je vytvořen v nepodporovaném datovém formátu nebo jej není možné zobrazit, rovněž není podatelnou přijat. Kontrola datového formátu je prováděna u všech komponent doručené zprávy. § 64 odst. 1 zákona 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů vyjmenovává přípustné datové formáty, které jsou určení původci povinni přijímat. Pro názornost jsou níže uvedeny nejfrekventovanější datové formáty (Kunt, Lechner, 2022, s. 92-94):

- PDF/A (Portable Dokument Format/Archive) - výstupní datový formát statických textových dokumentů a statických kombinovaných textových a obrazových dokumentů (ISO 19005);
- PNG (Portable Network Graphics) - výstupní datový formát statických obrazových dokumentů (ISO/IEC 15948);
- XML (Extensible Markup Language Document) - výstupní datový formát metadat, jimiž jsou opatřovány dokumenty v elektronickém systému spisové služby a výstupní datový formát pro databáze;
- MPEG-1 (Picture Experts Group Phase 1) - výstupní datový formát dynamických obrazových dokumentů (ISO/IEC 11172);
- GIF (Graphics Interchange Format) - výstupní datový formát dynamických obrazových dokumentů;
- MP3 (Music Protocol 3) - výstupní datový formát zvukových dokumentů.

Je možno přijímat i další datové formáty. O přijímaných formátech musí být veřejnost informována na úřední desce dané organizace. Obvykle veřejnoprávní původce připouští příjem datových formátů v širším rozsahu tak, jak jsou uvedeny v příloze č. 3 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování ISDS.

Evidence a označování dokumentů

Dle ZASS a vyhlášky 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky 283/2014 Sb., podléhají zaevidování pouze dokumenty mající úřední charakter. Doručené dokumenty (evidované jako „cizí“ či „cizí příchozí“) a dokumenty vzniklé z vlastí činnosti dané organizace (evidované jako „vlastní“ a „interní“) mají být

evidovány v evidenci dokumentů, která je součástí eSSL. Vedení dokumentu v eSSL má tu výhodu, že opravy a identifikace osob provádějících opravy jsou zpracovávány automaticky a o každém dokumentu se vedou údaje, mezi které patří jednoznačný identifikátor dokumentu obsahující pořadové číslo dokumentu, pod nímž je evidován v evidenci dokumentů, datum doručení dokumentu do dané organizace (případně čas doručení – dle daného předpisu) nebo jeho vytvoření v rámci organizace. Evidují se rovněž údaje o odesilateli, ale také údaje o kvantitě dokumentu (počet listů u dokumentů v listinné podobě nebo počet a druh příloh u dokumentů v nelistinné podobě).

NSESSS jasně stanovuje požadavky, které musí být při elektronické evidenci dokumentů splněny. Dokumentu v elektronické podobě je přidělen jednoznačný identifikátor (ID), který zůstává nezměnitelný po celý životní cyklus dokumentu v organizaci. Dokumentu může být přiděleno také číslo jednací, které je s dokumentem rovněž spojeno.

Jednoznačný identifikátor – je spojen s dokumentem v eSSL. Jedná se o automatizovanou funkci v rámci systému spisové služby. Identifikátor je jedinečný, nezaměnitelný a je zaznamenáván v metadatech. Jde o číselnou řadu generovanou systémem spisové služby formou alfanumerického kódu, v němž je zaznamenáno označení původce, případně jeho zkratka označení (Věstník Ministerstva vnitra – VMV čá. 57/2017 (část II), s. 5).

Číslo jednací – je rovněž jedinečné a je přiděleno každému zaevidovanému dokumentu. Struktura čísla jednacího je závazná a má informativní charakter. Číselná řada v evidenci dokumentů začíná dnem 1. ledna pořadovým číslem 1, končí dnem 31. prosince téhož roku, a to posledním pořadovým číslem daného roku. Číslo jednací se v eSSL generuje automaticky a to tak, aby byla zachována jeho jedinečnost a posloupnost (Sulitková, 2017, s. 91). Ve struktuře čísla jednacího se objevuje rok vytvoření, číselná či písmenná zkratka organizačního útvaru původce, vazba na iniciační dokument (rozlišovací číslo) atd. Charakter a tvorba čísla jednacího musí být uvedena ve spisovém řádu organizace.

Rozdělování a oběh dokumentu

Dokument musí být bezodkladně po zaevidování podatelnou předán příslušnému oddělení, které je určeno jeho zpracováním či vyřízením, případně přímo pověřenému zaměstnanci (Brom, 2013, s. 72). Proces rozdělování dokumentů a závazné postupy s tím

spojenými stanovuje spisový řád dané organizace a je zpracován v souladu s příslušnými nařízeními, zákony a vyhláškami na úseku archivnictví a spisové služby.

Rozdělování je distribuce pověření práce s dokumentem mezi uživateli spisové služby a automatizovanými činnostmi spisové služby za účelem vyřešení věci, které se dokument týká. Může se jednat o výměnu informací o řízení činností s dalšími systémy, jako je například workflow.

Oběh dokumentu může být řízen jak uživatelsky (tzn. danou oprávněnou osobou), tak automatizovaně pomocí předem definovaného postupu či procesu zpracování daného typu dokumentu. Oběh dokumentu je prováděn v souladu s nastavením uživatelských práv k danému dokumentu či spisu.

Během oběhu dokumentu je vytvářen transakční protokol, který je ve své podstatě auditním záznamem o práci uživatele v čase a životním cyklu dokumentu. Jak uvádí Kunt a Lechner (2017, s. 141-142), transakční protokol obsahuje záznam logovaných operací v systému spisové služby, které zaznamenávají důležité kroky v životním cyklu dokumentu, změny entity nebo eSSL. Rovněž umožňují dohledat, identifikovat a do jisté míry i rekonstruovat dokument. Z transakčního protokolu je možno vyčíst, kdo a kdy danou operaci provedl. NSESSL předkládá výčet minimálních informací, jejichž evidování musí být v transakčním protokolu zaznamenáno. Jedná se například o záznamy, jako je příjem dokumentu v elektronické podobě a jeho případné stornování (zničení), změny v přístupových oprávněních, změny skartačních režimů, přenos či zničení (odstranění) entit nebo změny v metadatech elektronických dokumentů, spisů, a to včetně typových, či věcných skupin.

Rozdělování dokumentů je proces, během kterého je určen příjemce, jemuž je předána práce s dokumentem pro jeho další zpracování. Funkce rozdělování může být prováděna jak automatizovaně, což se týká zpracování známých typů dokumentů (např. formulářová podání), tak uživatelsky, a to pověřeným pracovníkem, který pověří zpracováním konkrétní osobu.

Vyřizování

Vyřizování dokumentu je etapou, kdy probíhá praktická práce s dokumentem. Dochází k vyhotovování vlastních dokumentů dle kompetencí příslušného původce, a to v souladu s aktuálními platnými předpisy. Dokument je zakládán ho do spisu či typového spisu včetně ostatních dokumentů s tím spojených na vyřizovaný dokument. K etapě

vyřizování ZASS nespecifikuje požadavky, protože obsahově se jedná o kompetence příslušného původce či orgánu veřejné moci. Je pouze stanoveno, že odesílaný dokument má mít určité náležitosti, mezi které patří označení dané organizace (hlavička), číslo jednací, a to i doručeného dokumentu, podpis včetně jména a funkce osoby oprávněné k podpisu, datum podpisu, počet listů a příloh (Kunt, Lechner, 2022, s. 176-178).

Jak zmiňuje Kunt a Lechner (2022, s. 185-188), podepisování dokumentů je často v rámci organizace ošetřeno příslušnými vnitřními předpisy, a to řády či směrnicemi. Při podepisování analogového dokumentu se připojuje podpis v analogové podobě, tzn. vlastnoruční podpis. V takovém případě se často připojuje k vlastnoručnímu podpisu také otisk příslušného razítka. Při podepisování elektronického dokumentu se připojuje podpis v elektronické podobě, tzn. elektronický podpis. Jedná se o kvalifikovaný elektronický podpis a kvalifikovanou elektronickou pečeť.

Odesílání

Do etapy odesílání náleží veškerý proces od přípravy dokumentu k odeslání až po jeho opuštění dané organizace, resp. až po navrácení potvrzení o doručení (dodejky) či nabytí právní moci.

K odeslání dokumentů slouží výpravna, která je součástí podatelny. Na výpravnu jsou předávány dokumenty připravené k vypravení. To znamená dokumenty obsahující všechny potřebné náležitosti jako například vyhotovený a podepsaný dokument včetně všech náležitostí, mezi které se řadí počet příloh a listů příloh a další evidenční záznamy (Kunt, Lechner, 2022, s. 189).

Existují situace, kdy je třeba doložit doručení dokumentu adresátovi. K takovému účelu je určena dodejka (doručenka), která potvrzuje, že zásilka byla adresátovi řádně doručena. U doručovaného dokumentu v listinné podobě prostřednictvím poskytovatele poštovních služeb se po doručení a převzetí vrátí původci papírová dodejka (doručenka), u doručovaného dokumentu v elektronické podobě prostřednictvím ISDS, kdy je adresátovi odesílána datová zpráva, nebo prostřednictvím elektronické pošty, se původci vrátí elektronické potvrzení doručení (Kunt, Lechner, 2022, s. 189).

Ukládání

Ukládání je poslední etapa aktivní části životního cyklu dokumentu. Analogové dokumenty jsou ukládány ve spisovně, elektronické dokumenty v elektronické spisovně.

Kunt a Lechner (2022, s. 203-205) uvádějí, že se jedná o etapu, kdy již s dokumentem není aktivně pracováno, ale přesto dokument může být vyhledáván a předkládán původci. Rovněž na něm je ve vhodné době prováděno skartační řízení. Jasně také poukazují na problémy spojené s ukládáním a na sankce, které při chybném či nevhodném zacházení s ukládanými dokumenty a spisy původcům hrozí. U analogových dokumentů a spisů je zmiňován problém s vhodností prostor pro vytvoření spisovny. U elektronických dokumentů a spisů nastává problém s případným nesplněním požadavků na vhodný datový formát. Takový dokument musí být v rámci systému elektronické spisové služby do správného datového formátu převeden.

Vyřazování dokumentů

Vyřazování dokumentu je poslední etapou jeho životního cyklu. Tato etapa je spojena se skartačním řízením, výběrem archiválií a předáváním dokumentů vybraných za archiválie určenému archivu. Vyřazování dokumentů probíhá dle jejich potřebnosti a důležitosti z hlediska dokumentární hodnoty, tzn. vyřazovat dříve dokumenty nepotřebné pro danou organizaci a s nižší dokumentární hodnotou a zachování dokumentů s vyšší dokumentární hodnotou (např. právní či auditorské dokumenty). Kunt a Lechner (2022, s. 216-217) upozorňují, že se nejedná o jednorázový úkon zničení, ale o proces výběru bezcenných dokumentů určených ke skartaci a dokumentů hodnotných, tzn. určených pro trvalé uchování.

Dle § 5 ZASS jsou u orgánů veřejné moci za archiválie vybírány dokumenty s trvalou hodnotou významu a ve vztahu k funkci anebo postavení jejich původce.

Vyřazování je proces, během kterého dochází k přenosu dokumentů a spisů do archivu, přičemž dojde k jejich odstranění z eSSL, nebo jejich zničení.

4 Vlastní práce

4.1 Vliv aktuálního stavu legislativy na proces výkonu elektronických spisových služeb u veřejnoprávních původců

Z hlediska aplikační praxe je současná etapa vývoje vůbec tou nejsložitější etapou v dosavadní historii elektronizace spisových služeb, resp. elektronizace orgánů veřejné moci. Spisová služba je dynamicky se rozvíjející obor, který v současné době prochází významnou transformací. Jak již bylo zmíněno v předešlé části práce, mezi stěžejní dokumenty ovlivňující zásadním způsobem činnost a chod elektronického systému spisové služby v České republice patří:

- zákon č. 499/2004 Sb. o archivnictví a spisové službě, ve znění pozdějších předpisů;
- vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů;
- národní standard pro elektronické systémy spisové služby.

Četné připomínky z praxe poukazovaly na nesoulad NSESSL s vyhláškou a vyhlášky se ZASS. Objevila se tudíž potřeba a také snaha o narovnání vztahu NSESSL, vyhlášky a ZASS. Tyto tři opěrné body spisové služby musí být ve svém výkladu jednotné a musí tak být nastolena jasná a srozumitelná pravidla fungování eSSL.

4.1.1 Novelizace ZASS

ZASS je stěžejním legislativním dokumentem, který se týká elektronické spisové služby. Novelizací zákona mělo dojít k ucelení ukotvení eSSL. Jestliže bude na ZASS pohlíženo jako na zákon vymezující rámec eSSL, vyhláška č. 259/2012 Sb. je poté výkladovým materiálem a NSESSL je technickou normou obsahující popis jednotlivých bodů, které musí splňovat každá SW aplikace elektronické spisové služby.

V současnosti má eSSL před sebou tři časové milníky, během kterých by mělo dojít u většiny veřejnoprávních původců k implementaci eSSL, a to ve shodě s atestačními požadavky NSESSL. Tyto milníky zohledňují typy veřejnoprávních původců a jejich zvolený systém spisové služby. V původním znění DEPO měly veřejnoprávní původci uvést své eSSL do souladu se ZASS do 31. prosince 2023, ostatní určení původci pak do 31. prosince 2024. V tomto bodě je nutno připomenout, že se rapidně rozroste množina veřejnoprávních původců, kteří budou muset začít používat systémy spisové služby v elektronické podobě. To znamená, že povinnost používat pouze atestované systémy

elektronické spisové služby se dotkne velkého množství malých veřejnoprávních původců, kteří ukončí vedení svých spisových služeb v papírové podobě a budou muset přejít na eSSL, resp. na atestované eSSL. Mezi takové veřejnoprávní původce patří např. školy, státní podniky, zdravotní pojišťovny atd. Zákonem č. 89/2022 Sb., byl změněn zákon DEPO, čímž došlo k odložení účinnosti souladu eSSL se zákonem a byly stanoveny termíny atestací. Níže je uvedeno shrnutí třech časových milníků majících zásadní vliv na postup veřejnoprávních původců (tabulka 1):

Tabulka 1 Termíny a povinnosti vyplývající ze ZASS, vyhlášky a NSESSL ve vztahu k transformaci eSSL u veřejnoprávních původců

Termíny a povinnosti vyplývající ze ZASS, vyhlášky a NSESSL	
1. červenec 2023	Zahájení atestačního procesu eSSL, tzn. je možno začít podstupovat atestační proces v Atestačním středisku České agentury pro standardizaci. Týká se veřejnoprávních původců s eSSL a poskytovatelů eSSL.
1. červenec 2024	Zákaz nabízení/dodávání neatestovaných eSSL veřejnoprávním původcům. Nabízené, resp. dodávané eSSL musí být opatřeny atestem dle § 69e ZASS.
1. leden 2026	Začátek povinnosti používat eSSL u veřejnoprávních původců. Používané eSSL musí mít potvrzen soulad se ZASS, vyhláškou a NSESSL, tzn. musí být atestované u České agentury pro standardizaci.

Zdroj: Vlastní zpracování (2023)

Jak uvádí zákon DEPO, všichni veřejnoprávní původci budou mít od 1. ledna 2026 povinnost vést elektronickou spisovou službu. Nicméně fakticky mají veřejnoprávní původci na změnu svých systémů spisových služeb pouze dva a půl roku, protože požadavky na eSSL vydané závaznou formou NSESSL jsou účinné teprve od 1. července 2023. Nutně proto vyvstává ze strany odborné veřejnosti legitimní požadavek na upravení stanovených termínů. Tento podnět je Ministerstvem vnitra ČR akceptován a aktuálně je projednávána novelizace ZASS zahrnující mimo jiné právě posunutí termínů vztahujících se k eSSL. Přehled nově navrhovaných termínů je zobrazen v tabulce 2.

Tabulka 2 Přehled aktualizovaných termínů a povinností předpokládaných v novele ZASS ve vztahu k transformaci eSSL u veřejnoprávních původců

Přehled aktualizovaných termínů a povinností předpokládaných v novele ZASS	
1. leden 2025	Zákaz nabízení/dodávání neatestovaných eSSL veřejnoprávním původcům. Nabízené, resp. dodávané eSSL musí být opatřeny atestem dle § 69e ZASS.
1. leden 2027	Začátek povinnosti používat eSSL u veřejnoprávních původců. Používané eSSL musí mít potvrzen soulad se ZASS, vyhláškou a NSESSL, tzn. musí být atestované u České agentury pro standardizaci.

Zdroj: Vlastní zpracování (2023)

Prodloužení přechodových období je více než vítané. Delší období na implementaci veškerých změn, které proběhly, a ještě se chystají, může být bráno jako vstřícný krok jak směrem k dodavatelům a distributorům eSSL, tak i veřejnoprávním původcům samým. Zapracování všech změn a novinek v oblasti spisové služby je náročným technickým procesem. Je třeba po stránce technické všechny kroky připravit, naprogramovat, otestovat a zakomponovat do eSSL. Nesmí být opomenuta rovněž metodická rovina. Jedná se o velkou změnu v chodu veřejnoprávních organizací, kde eSSL spadá do páteřních systémů. Bude nutné vypracovat nové spisové a skartační řády, metodické postupy, ale hlavně naučit uživatele daných eSSL novým pracovním postupům. V přechodových obdobích musí rovněž eSSL projít zdárně atestačním procesem České agentury pro standardizaci a získat atestační ověření. Řada veřejnoprávních původců bude nucena své eSSL nově vysoutěžit formou veřejné zakázky. Vše potřebuje svůj čas, který snad bude s přijetím novely ZASS prodloužen. Jestli ovšem bude dostatečný, se teprve ukáže.

4.1.2 Novelizace vyhlášky č. 259/2012 Sb.

Dne 1. července 2023 vstoupila také v platnost novela vyhlášky č. 259/2012 Sb., jejímž záměrem bylo uvést do souladu vyhlášku a ZASS, resp. reagovat na změny uvedené v zákonu DEPO. K obsahovým změnám v ZASS ovšem nedošlo, tudíž změny uvedené v novele vyhlášky se staly opět pouze jejím přizpůsobením k NSESSL, což je předmětem četné odborné kritiky.

Novelizace vyhlášky obsahuje více než osmdesát změnových bodů, které se týkají všech částí životního cyklu dokumentu. U některých změn se jedná o formální drobnosti, jiné jsou ovšem opravdu zásadními změnami v práci s dokumenty. Tyto změny se promítají do nové verze NSESSL, jehož novelizace vstoupila v platnost rovněž 1. července 2023.

4.1.3 Novelizace vyhlášky č. 259/2012 Sb.

Jako druhý se o narovnání snaží NSESSL. Jak bylo již zmíněno, na NSESSL je pohlíženo částečně jako na technický dokument, který popisuje fungování eSSL právě v souladu s ZASS a vyhláškou č. 259/2012. Jeho opora a návaznost na ZASS a vyhlášku je nezbytný právě proto, že se jedná o dokument, podle něhož pracovníci spisové služby, informatici a vývojáři postupují za účelem implementace bodů NSESSL do jednotlivých elektronických spisových služeb.

Novelizovaný NSESSL je představován jako zcela nová technická verze národního standardu. NSESSS je složen z deseti kapitol (základní pojmy, příjem a evidence dokumentů, spisový a skartační plán a organizace spisů, odkazování mezi entitami, vyhledávání, výběr, znázorní a ztvárnění, ukládání a vřazování dokumentů, správa a bezpečnost, rozhraní pro propojení informačních systémů spravujících dokumenty, metadata a dokumentace životního cyklu).

Národní standard se mimo jiné zaměřuje na:

- úpravu a revizi užívaných pojmů ve vyhlášce č. 259/2012 Sb., případně vypuštění pojmů (např. zásilka, redakce), které jsou buď přežité nebo nadbytečné či ve svém významu jasné (např. webová služba, verze);
- redefinuje pojem a význam hesla komponenta – pojem komponenta se nově používá pouze u digitálního dokumentu;
- zavádí a vysvětluje kontejnerové datové formáty;
- zabývá se revizí celého životního cyklu dokumentu;
- specifikuje a podrobněji popisuje typový spis a práci se spisy;
- zabývá se jmenným rejstříkem;
- specifikuje požadavky směrem k samostatným evidencím dokumentů a jejich propojení s elektronickými systémy spisových služeb.

4.1.4 Hodnocení aktuálního stavu legislativy na proces výkonu elektronických spisových služeb u veřejnoprávních původců

Je nutné konstatovat, že některé požadavky popsané v NSESSL přesahují požadavky ZASS a vyhlášky. To znamená, že požadavky uvedené v NSESSL jsou obsáhlejší než v ZASS či vyhlášce. Ačkoli je NSESSL pouze technickou normou a nikoli výkladovým předpisem, přesto obsahuje specifičtější požadavky, než stanovuje ZASS a vyhláška. Vhodným příkladem takové praxe je práce se spisy. ZASS například říká, že se všechny dokumenty týkající se téže věci při vyřizování dokumentů spojí ve spis. Již ovšem nehovoří o druzích spisu, řazení dokumentu ve spisu atd. Vyhláška uvádí, že dokument evidovaný v základní evidenční pomůcce se nejpozději před zahájením vyřizování vloží do spisu a popisuje náležitosti, které má spis obsahovat. Také rozlišuje spis a typový spis. NSESSL ale již požaduje povinné vyřizování dokumentů ve spisu. Dokument má být do spisu vložen hned po přijetí či vytvoření. Dokonce povoluje vytvoření prázdného spisu, tzn. spisu bez dokumentu, což z praktického hlediska nedává příliš smysl.

Jak je na příkladu vytváření spisu patrno, nedochází k narovnání ZASS, vyhlášky a NSESSL, ale naopak k jasnému přesahu požadavků NSESSL nad rámec ZASS a vyhlášky

4.2 Spisová služba veřejnoprávního původce – Celní správa České republiky

Celní správa České republiky (dále jen „Celní správa ČR“) je správním orgánem a současně bezpečnostním sborem, který zajišťuje výkon stanovených kompetencí v oblasti správy cel a některých daní, včetně dalších svěřených činností (zákon č. 17/2012 Sb., o Celní správě České republiky). Zabývá se dohledem nad zbožím v rámci celního území Evropské unie. Do její gesce spadá velká řada kompetencí, jako je například:

- celní řízení a správa cla – tj. dohled a kontrola nad zbožím dováženým, prováženým a vyváženým, zajištění celního dluhu, dodržování obchodně politických opatření České republiky a Evropské unie, zákazy a omezení při dovozu, vývozu či tranzitu, pátrání po zboží protiprávně dovezeném či vyvezeném;
- správa spotřebních a energetických daní – tj. správa spotřebních daní, správa registru prodejců pohonných hmot; správa daní ze zemního plynu a některých dalších plynů, z pevných paliv a daň z elektřiny;
- dělená správa – tj. vybírání a vymáhání peněžitých plnění (např. pokut) uložených jiným správním úřadem v řízení podle správního řádu;

- ochrana práv duševního vlastnictví, přírody (hlavně exempláře CITES), předmětů historické a kulturní hodnoty;
- kontrola přepravy omamných a psychotropních látek;
- kontrola v oblasti silniční dopravy – tj. vážení nákladních vozidel, dálniční známky, mýtné, nebezpečné náklady;
- kontrola zaměstnávání cizinců – ze zemí i mimo země Evropské unie;
- kontrola provozování hazardních her;
- trestní řízení – tj. kompetence vyplývající z postavení celních orgánů jako orgánů činných v trestním řízení u trestných činů, kdy byly porušeny předpisy v oblasti celní a daňové.

Uvedený výčet naznačuje složitost a mohutnost celého systému. Celní správa ČR se opírá o šest procesních předpisů, kterými jsou daňový řád (zákon č. 280/2009 Sb.), správní řád (zákon č. 500/2004 Sb.), kontrolní řád (zákon č. 255/2012 Sb.), trestní řád (zákon č. 141/1961 Sb.), občanský soudní řád (zákon č. 99/2016 Sb.) a rovněž jsou procesní ustanovení uvedená v zákoně č. 17/2012 Sb., o Celní správě České republiky. Z výše uvedeného je možné vyvodit, že eSSL v rámci Celní správy ČR je široký a velmi složitý komplex, který je již od roku 2008 vyvíjen v souladu se zákonnými požadavky eSSL, ale také s požadavky ostatních agend spadajících do kompetencí celní správy. Informační systém správy dokumentů Celní správy ČR představuje sofistikovaný systém aplikací, evidencí, databází a formulářových řešení, přičemž velký důraz je kladen na kyberbezpečnost. Z výše uvedeného vyplývá, že eSSL Celní správy ČR je systém velmi provázaný, ale také systém, u kterého se přísně dbá na bezpečnost ohledně dat, jejich získávání a přístupu. Systém není rigidní, stále se vyvíjí, dotváří se nové a zdokonalují se stávající aplikace. Právě z toho důvodu byl vybrán pro přiblížení toho, jaké důsledky na eSSL mohou mít nové požadavky v oblasti eSSL u veřejnoprávních původců, kteří se elektronizací SSL zabývají už dlouho a jejichž eSSL není možno jednoduše přesoutěžit či nově modulárně řešit.

4.2.1 Architektura SW aplikací pro správu dokumentů v Celní správě ČR

Páteřním systémem v architektuře aplikací pro správu dokumentů Celní správy ČR je aplikace dodávaná společností TranSoft a.s. nazývající se Elektronická spisová agenda (zkratka „eSAT“). Jedná se o centralizovanou aplikaci s webovým rozhraním, kterou využívají všechny orgány celní správy. Každý orgán Celní správy ČR (Generální ředitelství

cel a patnáct celních úřadů) je samostatným veřejnoprávním původcem se samostatnou podatelnou, výpravnou a datovou schránkou, přičemž eviduje dokumenty ve své vlastní řadě čísel jednacích.

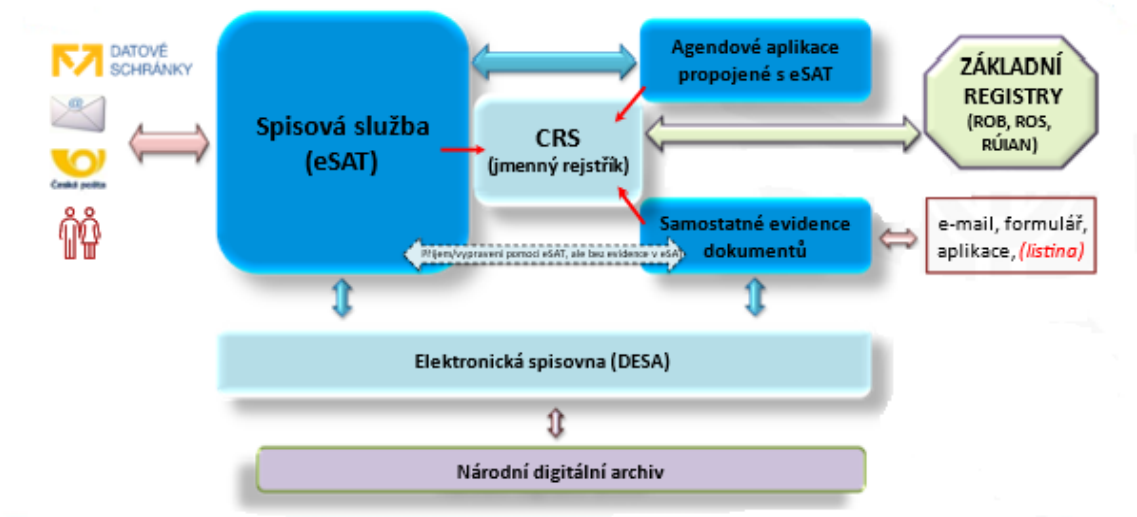
Tato aplikace stála při počátku elektronizace Celní správy ČR, díky čemuž prošla řadou úprav a vylepšení tak, aby bezezbytku plnila jak požadavky zákonné, tak provozní požadavky ze strany Celní správy ČR. Za více jak patnáct let fungování se stal eSAT nedílnou součástí architektury SW aplikací Celní správy ČR. Jeho provázanost s ostatními specifickými a často ojedinělými SW aplikacemi svého druhu je tak markantní, že případná výměna spisové služby není snadno proveditelná. Je nutné připomenout, že v Celní správě ČR existuje díky řadě specifických a ojedinělých kompetencí značné množství rozličných aplikací, které jsou vytvářeny právě jen pro potřeby Celní správy ČR.

Je možno stanovit základní funkce aplikace eSAT, které jsou využívány všemi uživateli aplikace bez rozdílu jejich pracovní pozice. Základní funkce aplikace eSAT jsou:

- komunikace s ISDS a elektronickou podatelnou;
- správa dokumentů a spisů – digitálních, analogových;
- vnitřní oběh dokumentů včetně schvalovacího procesu;
- práce s elektronickými spisy – věcnými, typovými (daňovými, správními, kontrolními a jinými pro potřebu organizace);
- správa spisového a skartačního plánu.

Níže je znázorněno schéma informačního systému správy dokumentů v Celní správě ČR včetně popisu jednotlivých částí schématu (obrázek 1):

Obrázek 1 Schéma informačního systému správy dokumentů v Celní správě ČR



Zdroj: Vlastní zpracování (2023)

Elektronický systém spisové služby (eSSL)

Aplikace Spisová agenda Celní správy ČR slouží ke správě doručených (cizích), odeslaných (vlastních) a interních dokumentů a k ukládání elektronických dokumentů. Základním požadavkem na aplikaci je zajištění evidence dokumentů a dalších souvisejících činností. Aplikace slouží k výkonu spisové služby dle platných zákonů, prováděcích předpisů, NSESSL a příslušných vnitřních předpisů Celní správy ČR.

Aplikace je řešena jako centrální intranetová aplikace. Provoz je tedy plně zajištěn v centru a pro přístup k aplikaci slouží pouze webový prohlížeč. Přístup jednotlivých uživatelů do aplikace je řešen prostřednictvím Active Directory, uživatelé se tedy nemusejí přihlašovat k aplikaci samotné, ověření uživatele probíhá na základě jeho přihlášení v pracovní stanici či prostřednictvím čipové karty. Pro spuštění aplikace stačí pouze zadat příslušnou adresu do webového prohlížeče.

Přístupová práva jednotlivých uživatelů jsou nastavena na dvou úrovních. První úrovní je již zmíněný systém Active Directory, ve kterém je možné určit, kteří uživatelé mají do aplikace přístup, a kteří mají oprávnění provádět administraci aplikace. Druhou úrovní přístupových práv jsou uživatelské role, čímž je míněna definice funkcí, které může uživatel v aplikaci využít. Uživatelské role jsou nastavovány přímo v aplikaci.

Součástí aplikace je rovněž komunikační rozhraní, které umožňuje automatizovaný zápis dokumentů i zprostředkovaně prostřednictvím jiných aplikací provozovaných v Celní správě ČR. Jde o programové rozhraní implementované dle standardu Web Services. Toto komunikační rozhraní slouží zejména k jednotné evidenci dokumentů a k jednotnému přidělování čísel jednacích.

Dalšími aplikacemi, které využívají komunikačního rozhraní ve vztahu k páteřnímu systému spisové služby, je Centrální registr subjektů (tzv. „CRS“), který plní funkci jmenného rejstříku v organizaci, následně samostatné a zdrojové evidence a elektronická spisovna (viz obrázek 1).

Centrální registr subjektů

Jak již bylo zmíněno, CRS plní v Celní správě ČR funkci jmenného rejstříku. V rámci této aplikace probíhají dotazy do Základních registrů.

Zároveň se změnilo postavení jmenného rejstříku v eSSL – spisová služba, samostatné evidence dokumentů i agendové aplikace propojené s eSSL jsou napojeny na jmenný rejstřík a přes něj využívají informace základních registrů (viz obrázek 1).

V Centrálním registru subjektů je rovněž spravován vlastní interní adresář neregistrovaných subjektů v Základních registrech (např. zahraniční subjekty). Tento adresář je editovatelný, ale pouze administrátorským, nikoliv uživatelským přístupem, čímž se zabrání nahromadění více shodných záznamů v editovatelné části jmenného rejstříku.

Elektronická spisovna

Funkci elektronické spisovny, resp. důvěryhodné elektronické spisovny, zastává v Celní správě ČR systém od společnosti ICZ a. s., který se nazývá ICZ DESA. Jedná se o systém garantující důvěryhodné uchovávání elektronických dokumentů v dlouhodobém horizontu, a to za dodržování všech legislativních pravidel. ICZ DESA garantuje používání archivních standardů a rovněž tak zachování dlouhodobé čitelnosti, neměnnosti a věrohodnosti dokumentů a spisů.

V případě Celní správy ČR plní ICZ DESA funkci dlouhodobého úložiště, které zajišťuje platnost, čitelnost a uchování elektronických dokumentů v dlouhodobém horizontu, a to včetně jejich zachování validity při elektronickém skartačním řízení. Následně disponuje mechanismy k vytváření skartačních rozhodnutí a zajišťuje snadné předávání archiválií nadřízenému archivu. Po dokončeném skartačním řízení zajistí zničení

vybraných dokumentů a spisů. Ve střednědobém horizontu zůstává pro dokumenty úložištěm aplikace eSAT.

Agendové aplikace propojené s eSSL

Příkladem agendové aplikace provozované Celní správou ČR je Modul exekucí a dražeb (tzv. MED), která není samostatnou evidencí podle § 8 odst. 2 vyhlášky č. 259/2012 Sb. Rozdíl oproti samostatné evidenci dokumentů spočívá v tom, že ačkoliv se správa dokumentu (nebo též část jeho životního cyklu) odehrává v agendové aplikaci, zákonné náležitosti zajišťuje pro tyto dokumenty základní aplikace spisové služby, eSAT. Zejména se jedná o přidělení čísla jednacího v postavení agendového identifikátoru, náležitosti příjmu, vypravení, uložení dokumentu.

Samostatné evidence dokumentů

Samostatné evidence dokumentů vedené v elektronické podobě musí být v souladu s požadavky stanovenými NSESSL a vyhláškou. Jejich shodu s požadavky NSESSL deklaruje výrobce aplikací prohlášením o shodě.

Samostatná evidence dokumentů zajišťuje celý životní cyklus dokumentu mimo základní evidenční pomůcku spisové služby. Samozřejmě existuje technologické spojení mezi spisovou službou a samostatnou evidencí dokumentů prostřednictvím aplikačního rozhraní zejména pro potřeby příjmu a vypravení dokumentu, neboť pouze základní evidenční pomůcka (eSAT) je propojená s ISDS a s ePodatelnou. Pro zajištění shody se zákonnými požadavky opatří eSAT přijatou zprávu prvotním identifikátorem a předá ji prostřednictvím aplikačního rozhraní k dalšímu zpracování. Ostatní úkony jsou již prováděny v rámci samostatné evidence dokumentů.

Dokument zaevidovaný v samostatné evidenci dokumentů se označuje evidenčním číslem ze samostatné evidence dokumentů. Evidenční číslo ze samostatné evidence dokumentů musí splňovat minimálně podmínky stanovené pro jednoznačný identifikátor a musí dále obsahovat název samostatné evidence dokumentů a pořadové číslo. Strukturu evidenčního čísla a další podmínky využití samostatné evidence dokumentů z pohledu spisové služby upřesňují dotčené odborné útvary Celní správy ČR vnitřním aktem řízení.

Níže následuje výčet samostatných evidencí dokumentů vedených v elektronické podobě, ve kterých vznikají a jsou uchovávány dokumenty pod vlastním evidenčním číslem, bez evidence v eSAT, a které komunikují bez použití datových schránek, zpravidla pomocí

technického zařízení umožňující dálkový přístup. Tyto samostatné evidence dokumentů jsou považovány ve smyslu vyhlášky č. 259/2012 Sb. vedle eSAT za součást elektronického systému spisové služby Celní správy ČR. Samostatnou evidencí dokumentů jsou v Celní správě ČR jen ty evidence, které takto stanovuje Spisový řád Celní správy ČR. Jedná se o tyto samostatné evidence dokumentů:

- eVývoz (ECS) – evidence a kontrola celního řízení ve vývozu s rozsáhlejší elektronickou komunikací zúčastněných subjektů v rámci Evropské unie;
- eDovoz (ICS) – evidence a kontrola celního řízení v dovozu s elektronickou komunikací v rámci Evropské unie;
- NCTS/TIR – evidence a kontrola tranzitních operací;
- EMCS (SPD/EVV) – podpora sledování přepravy zboží podléhajícího zákonu č. 353/2003 Sb., o spotřebních daních;
- AVIS^{ME} – Automatizovaný Vnitřní Informační Systém – evidence financování činnosti Celní správy ČR v rozsahu stanoveném správcem;
- Elektronické trestní řízení (ETŘ) – evidence dokumentů pro výkon agendy trestního řízení;
- Personální informační systém Ginis (PIS Ginis) – podpora personální evidence včetně výpočtu mzdových nároků v rozsahu stanoveném správcem.

4.2.2 Vybrané aspekty životního cyklu dokumentu v Celní správě ČR

Z hlediska aplikační praxe nastávají v životním cyklu dokumentu určité okamžiky, které mohou být z hlediska dalšího zpracování poměrně problematické. Níže byly vybrány body, kterým každý veřejnoprávní původce, zejména s ohledem na aktuální legislativu, věnuje zvýšenou pozornost.

Výstupní datový formát zpracovávaných dokumentů

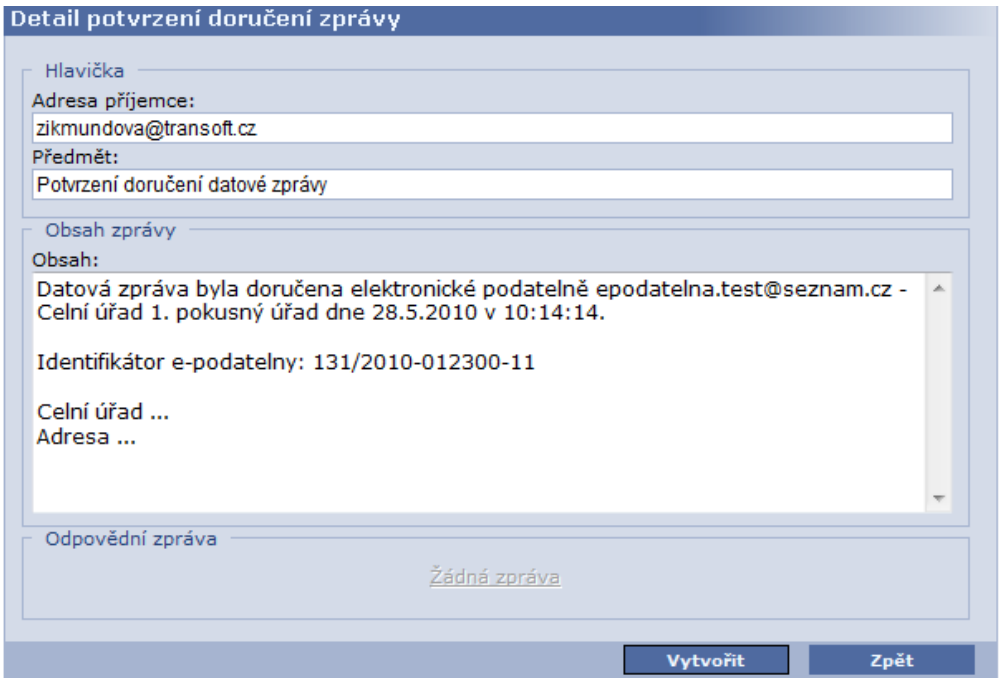
Příjmu dokumentů do organizace je věnována značná pozornost. Veřejnoprávní původce má povinnost přijímat stanovené typy dokumentů (např. PDF, PDF/A, doc/docx, html/htm, xls/xlsx atd.). Ovšem je na úvaze a schopnosti dané organizace, zda bude na podacím místě přijímat rovněž typy dokumentů jiných formátů, tzn. nad rámec stanovený ZASS. Praktické a účelné je přijímat formáty nejméně v rozsahu podle přílohy č. 3 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování ISDS.

Na úřední desce veřejnoprávního původce (elektronické i fyzické) musí být uvedeny přijímané formáty podání. Jestliže odesilatel nedodrží tuto podmínku, organizace může odmítnout dokument přijmout a zaevidovat, o čemž musí být odesílatel informován.

Povinností veřejnoprávního původce tedy není přijmout jakýkoliv typ podání, proto je nejvýhodnější, aby kontrola na datové formáty byla nakonfigurována v eSSL v modulu podatelna, a to ve shodě se zákonnými požadavky, resp. s rozšířenými typy přijímaných formátů uvedených na úřední desce dané organizace. Jestliže dokument neprojde kontrolou, resp. poruší podmínku týkající se přijímaného typu dokumentu, bude danou organizací odmítnut hned v podatelně a nebude zaevidován.

V praxi nejčastěji tato situace nastává při zpracování e-mailů. V případě úspěšného zaevidování příchozí e-mailové zprávy je automaticky zobrazen formulář pro vytvoření potvrzení o doručení zprávy (obrázek 2). V případě úspěšného zaevidování příchozí e-mailové zprávy je automaticky zobrazen formulář pro vytvoření potvrzení o doručení zprávy.

Obrázek 2 Detail potvrzení o doručení e-mailové zprávy



Zdroj: Celní správa ČR, eSAT (2023)

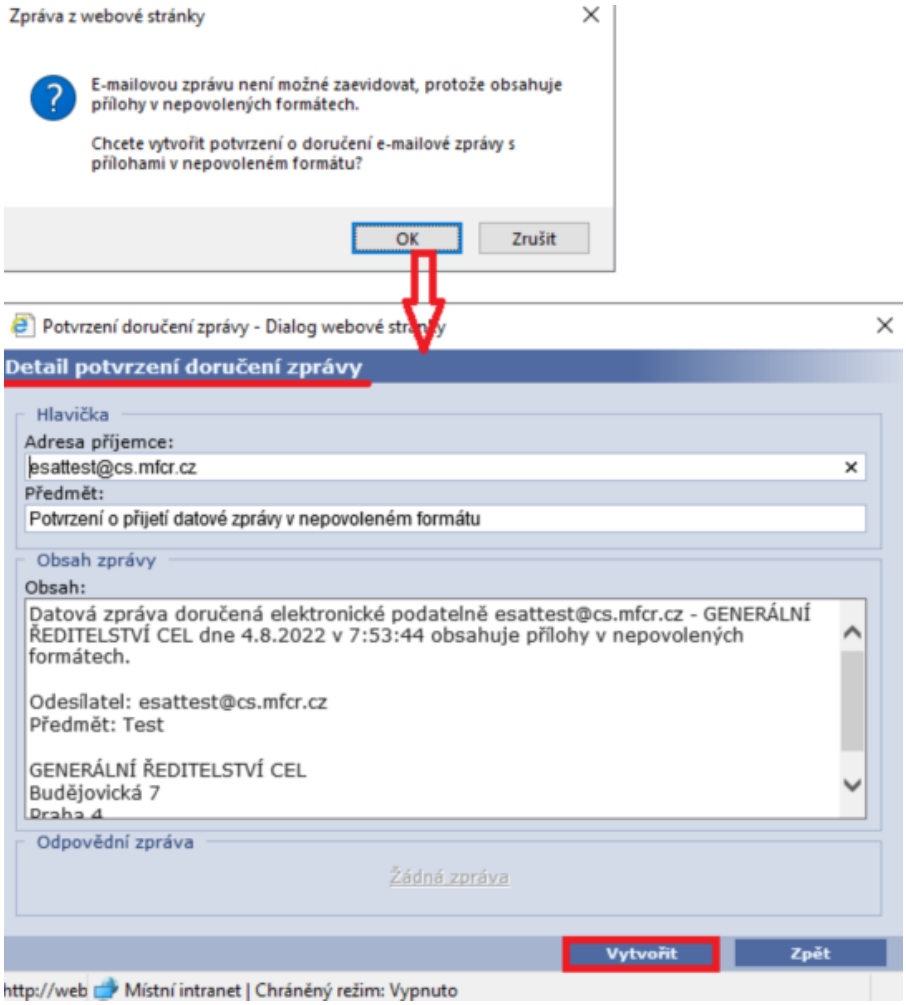
Dokument vytvořený z e-mailové zprávy má již nastavený typ dokumentu „cizí (příchozí)“, dále je přednastaven způsob a datum doručení. E-mailová adresa odesílatele je předvyplněna na základě údajů z e-mailové zprávy.

V případě komunikace pomocí e-mailu se ovšem často také stává, že je do e-mailové schránky Celní správy ČR doručena nevyžádaná zpráva nebo zpráva v nesprávném či poškozeném formátu. Taková zpráva nemusí být zaevidována a může být v aplikaci eSAT pouze označena jako nezaevidovaná. Zpráva následně není zobrazena ve výchozím nastavení vyhledávání příchozích e-mailových zpráv. Nezaevidovaná zpráva však zůstává v aplikaci eSAT po určitou dobu uchována a v případě chybného označení je možné ji opětovně zařadit mezi přijaté zprávy a následně zaevidovat.

Aplikace neovlivňuje žádným způsobem počet potvrzujících zpráv, ani jejich obsah. Pro případ, kdy je příchozí zpráva zaevidována, nabízí aplikace předvyplněný text potvrzovací zprávy s údaji o přiděleném čísle jednacím a časovém údaji přijetí zprávy ePodatelnou. Stejnou funkci je možné využít i pro případ zaslání oznámení o nepovoleném formátu v příchozí e-mailové zprávě apod.

Při příjmu e-mailových zpráv provádí aplikace kontrolu povolených datových formátů příloh. Aplikace eSAT nepovolí zaevidování e-mailových zpráv, které obsahují přílohy v nepovolených formátech. Při pokusu o zaevidování takové e-mailové zprávy zobrazí aplikace upozornění na možnost vytvoření potvrzení o doručení (obrázek 3). Potvrzení je vytvářeno obdobným způsobem, jako při zaevidování e-mailové zprávy, ovšem s odlišným textem potvrzení. Po úspěšném vytvoření a odeslání potvrzení o doručení zprávy v nepovoleném formátu je zpráva označena jako nezaevidovaná.

Obrázek 3 Zpráva eSAT o obdržení e-mailové zprávy v nepovoleném formátu



Zdroj: Celní správa ČR, eSAT (2023)

Dalším významným bodem je povinnost převést dokument při příjmu podání rovnou do výstupního datového formátu v souladu s ustanovením § 23 vyhlášky č. 259/2012 Sb. Tato problematika se týká hlavně e-mailů a listinných dokumentů doručených veřejnoprávnímu původci.

Elektronický dokument může být doručen do e-mailové schránky referenta, tzn. mimo podací místo, kterým by v tomto případě byla ePodatelna. Příslušný pracovník musí zajistit, že dokument v nevýstupním formátu (např. formát .eml) bude převeden do formátu výstupního. U e-mailové komunikace je třeba, aby byl daný e-mail předán na podatelnu k zaevidování. Podatelna při evidování zajistí jeho převod do výstupního datového formátu, např. PDF/A. Pro zachování všech metadat je ale nutné, aby byla e-mailová zpráva přeposlána na podatelnu v původním znění bez úprav. To znamená, že doručený e-mail musí být přeposlán příslušným zaměstnancem přímo na podatelnu k zaevidování. Bude tak

učiněno podání, dokument bude přijat do eSSL se všemi nutnými náležitostmi (číslo jednací, metadata, vhodný datový formát atd.).

U listinného dokumentu je nutné takto získaný dokument (např. záznam z šetření atd.) doručit na podatelnu fyzicky. Listinný dokument bude naskenován do systému eSSL a fyzicky opatřen štítkem s QR kódem. V eSSL bude opatřen číslem jednacím, časovým razítkem a v metadatech si ponese dané informace např. o způsobu a datu doručení.

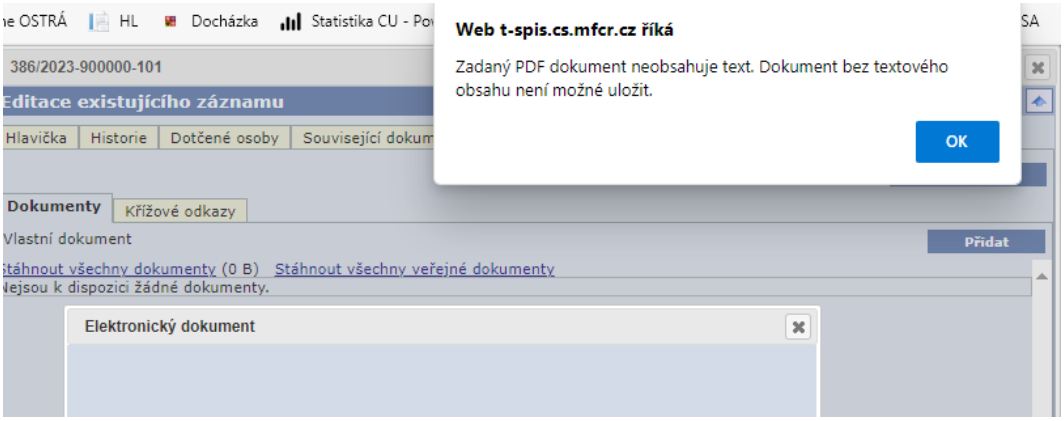
Strojově čitelná vrstva

Novelizací vyhlášky č. 259/2012 Sb. byla stanovena povinnost vkládat do spisové služby textové komponenty vzniklé z vlastní činnosti pouze ve formě strojově čitelné vrstvy. Strojově čitelná vrstva neboli OCR (Optical Character Recognition) umožňuje optické rozpoznávání znaků. Jedná se o metodu, která umožňuje digitalizaci tištěných textů, s nimiž pak lze pracovat jako s běžným elektronickým textem. K této problematice vydal Odbor archivní správy a spisové služby Ministerstva vnitra ČR dne 27. ledna 2022 stanovisko (čj. MV- 23406-1/AS-2022), ve kterém se uvádí: *„Ministerstvo vnitra navrhlo výše popsanou úpravu vyhlášky z praktických důvodů, zejména, aby usnadnilo přístup k dokumentům osobám se zdravotním postižením, zefektivnilo zpracovávání dokumentů zejména po technické stránce a zamezilo původcům vykonávajícím spisovou službu v elektronické podobě nesprávným způsobem vytvářet digitální dokumenty (bez textové vrstvy)“.*

V praxi je ovšem tato povinnost terčem časté kritiky, neboť se ukazuje, že existuje nemálo případů, kdy je tento požadavek nerealizovatelný. Často je veřejnoprávní původce nucen do vlastního čísla jednacího vložit dokumenty stažené z veřejně přístupného rejstříku, které ovšem textovou vrstvu samy neobsahují – např. Celní správa ČR v postavení správce daně není oprávněna vyžadovat od subjektů informace, které lze získat z Katastru nemovitostí, anebo Obchodního rejstříku.

Kvůli problémům se správným vytvářením strojově čitelné vrstvy byla v Celní správě ČR nasazena její kontrola v aplikaci eSAT. Textové dokumenty bez strojově čitelné vrstvy jsou aplikací eSAT blokovány a není možné je do aplikace eSAT vložit (obrázek 4).

Obrázek 4 Detail informace o dokumentu bez strojově čitelné vrstvy



Zdroj: Celní správa ČR, eSAT (2023)

Kontrola podpisu v rámci schvalovacího procesu

Na základě nařízení eIDAS (viz výše) je nutné opatřit elektronický dokument kvalifikovaným elektronickým podpisem, případně kvalifikovanou pečetí, a časovým razítkem.

Celní správa ČR, resp. aplikace eSAT, kontroluje při podepisování elektronických dokumentů kvalifikované certifikáty pracovníků, které mají na své zaměstnanecké čipové kartě. eSAT při podpisu vybírá a nabízí jen kvalifikovaný podpis.

V závislosti na nastavení aplikace je při vypravení elektronického dokumentu vyžadováno připojení kvalifikovaného elektronického podpisu. K vloženým elektronickým dokumentům lze připojovat elektronické podpisy a časová razítka. V případě podpisu elektronického dokumentu ve formátu PDF jsou elektronické podpisy vkládány přímo do dokumentu. V případě ostatních formátů jsou vytvářeny externí podpisy.

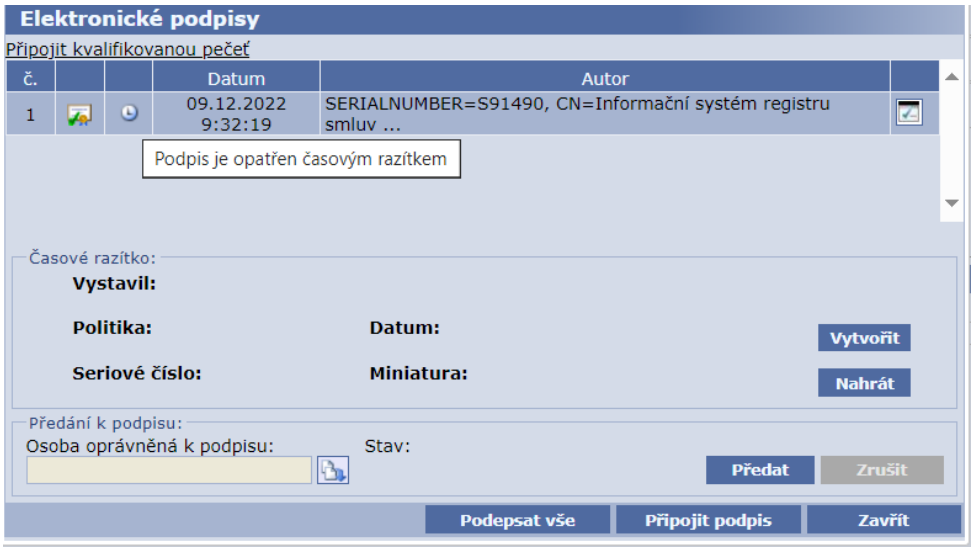
V praxi to znamená, že oprávněný uživatel cíleně připojuje k elektronickému dokumentu podpis, a to kvalifikovaný elektronický podpis umístěný na jeho zaměstnanecké čipové kartě. Po připojení elektronického podpisu, tzn. po elektronickém podepsání dokumentu, je možno v aplikaci eSAT zobrazovat údaje o podepsání a použitém kvalifikovaném certifikátu (obrázek 5). Zároveň je dokument opatřen časovým razítkem (obrázek 6).

V závislosti na nastavení aplikace nemusí být dostupná funkce připojení elektronického podpisu u dokumentů, které jsou již opatřeny kvalifikovanou pečetí.

Obrázek 5 Dialogové okno – elektronický dokument obsahující platný kvalifikovaný podpis + detail podpisu

Zdroj: Celní správa ČR, eSAT (2023)

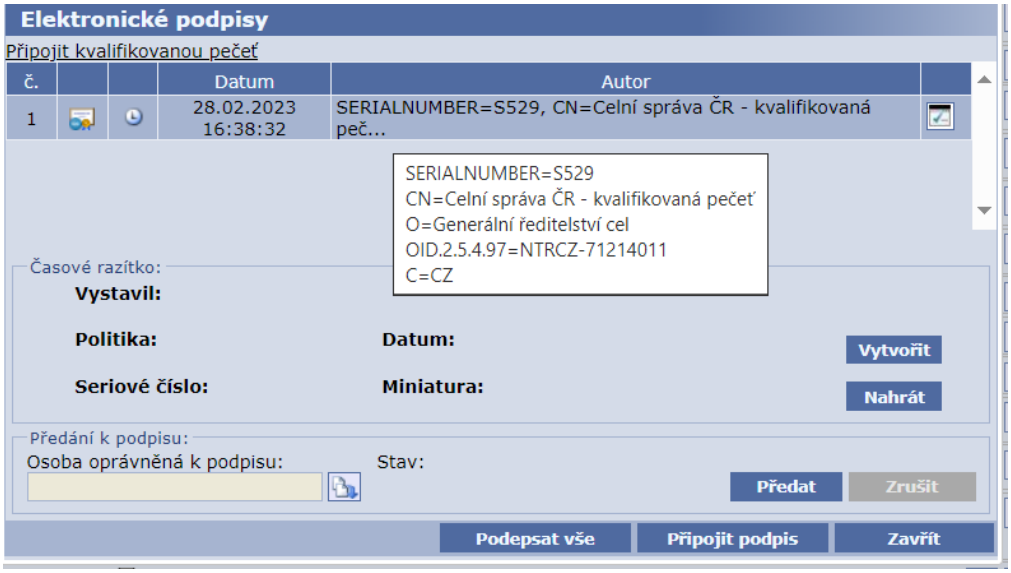
Obrázek 6 Dialogové okno – elektronický dokument obsahující časové razítko



Zdroj: Celní správa ČR, eSAT (2023)

V případě, že je součástí vypravovaného dokumentu příloha zkopírovaná z jiného dokumentu, umožňuje aplikace v některých případech použití kvalifikované pečeti namísto použití osobního kvalifikovaného elektronického podpisu (obrázek 7). Tato funkčnost je dostupná pouze u elektronických dokumentů, které nejsou podepsané a zároveň byly doručeny jako součást příchozího elektronického podání (např. jako příloha datové nebo e-mailové zprávy). V takových případech aplikace umožňuje v seznamu elektronických kvalifikovaných prostředků použít funkci „Připojit kvalifikovanou pečeť“.

Obrázek 7 Dialogové okno – elektronický dokument obsahující kvalifikovanou pečeť



Zdroj: Celní správa ČR, eSAT (2023)

Ztotožnění ve jmenném rejstříku

Povinnou součástí spisové služby je jmenný rejstřík. V Celní správě ČR je jmenným rejstříkem samostatná aplikace Centrální registr subjektů. Důležitost a potřebnost jmenného rejstříku, resp. ztotožnění subjektů přes jmenný rejstřík, je např. při využívání Daňové informační schránky, která byla jako prostředek komunikace mezi subjektem a správcem daně ustanovena daňovým řádem (zákon č. 280/2009 Sb., ve znění pozdějších předpisů). Prostřednictvím Daňové informační schránky může daňový subjekt získávat informace o něm shromažďované ve spisu a na osobním daňovém účtu. Rovněž je možno přes Daňovou informační schránku činit podání.

Elektronickou komunikaci mezi Celní správou ČR a subjekty zajišťuje cPortál, který je obdobou Daňové informační schránky. Hlavní myšlenkou cPortálu je zprostředkování jednoduché, rychlé a pohodlné komunikaci včetně podání a vyřízení žádostí. Na cPortál jsou napojeny klientské aplikace (např. elektronické celní prohlášení, přeplatky a nedoplatky subjektů), prostřednictvím kterých mohou subjekty vyřizovat podání vůči Celní správě ČR.

Ztotožnění subjektu ve jmenném rejstříku probíhá tak, že je během procesu ztotožnění vyslán dotaz do systému Základních registrů, kde je provedeno vyhledání dané osoby či subjektu v registrech.

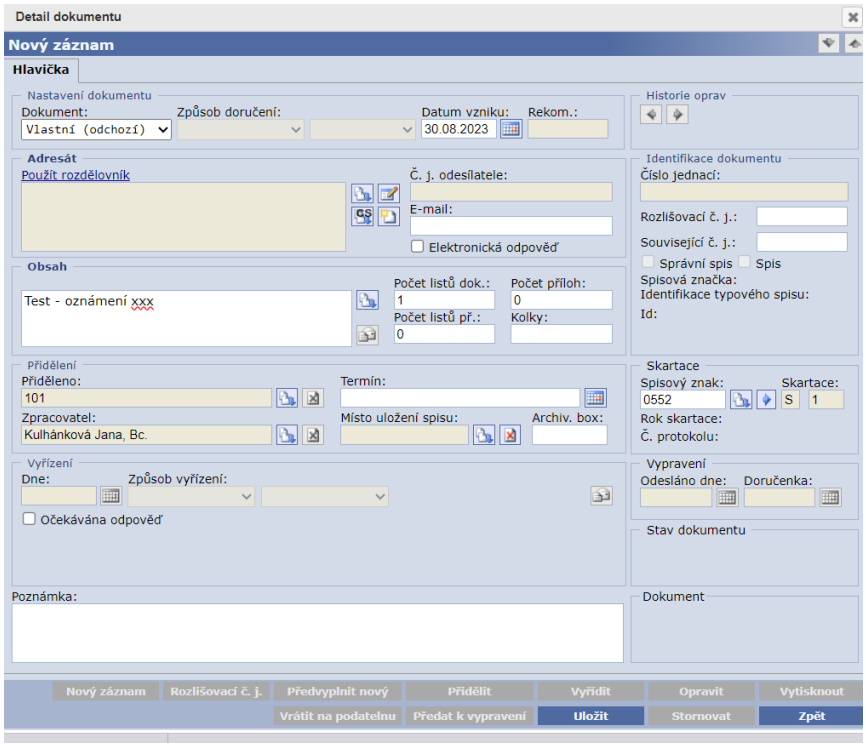
V návaznosti na změnu postavení jmenného rejstříku v eSSL došlo ke změně a zpřesnění pracovních postupů zaměstnanců Celní správy ČR při vytváření dokumentu. Již není možné v prvním kroku zadat jméno adresáta, a následně v dalších krocích teprve obsah věci a další atributy. Nyní již v prvním kroku vytváření dokumentu musí nejprve referent vyplnit obsah dokumentu (obrázek 8) a následně vyhledat adresáta ve jmenném rejstříku (obrázek 9). Až poté mu je spisovou službou vygenerováno číslo jednací. Důvodem tohoto postupu je zaznamenání uživatelského dotazu včetně identifikace uživatele (číslo jednací, osobní číslo uživatele) i na straně Základních registrů, nikoliv pouze v aplikaci Centrálního registru subjektů (tzn. jmenného rejstříku Celní správy ČR).

Jmenný rejstřík nahradil interní adresáře ve spisové službě a dalších evidencích. V praxi to znamená, že je potřeba podstoupit několik kroků ke ztotožnění uživatele. Při doručení dokumentu veřejnoprávnímu původci je vhodné hned na vstupu, tzn. v podatelně, ztotožnit odesílatele ve jmenném rejstříku. U datové zprávy je ztotožnění nejsnazší, protože se ztotožnění provede ověřením identifikátoru datové schránky a může probíhat automatizovaně na pozadí systému eSSL. U listinného dokumentu je ztotožněn odesilatel dle údajů, které uvedl v dokumentu. Vzhledem k tomu, že se předpokládá interakce mezi

odesilatelem a veřejnoprávním původcem, je pravděpodobné, že listinný dokument bude opatřen potřebnými identifikačními údaji (jméno, příjmení, adresa, datum narození aj.). Pravděpodobně nejčastěji nastává problém ztotožnění odesilatele při přijetí e-mailového podání, kdy verifikační údaje jsou často nedostačující. V některých případech vyplynou z obsahu textu sdělení, v jiných ovšem nikoli. Ztotožňování takových druhů e-mailových podání by měl proto provádět příslušný referent zabývající se řešením daného podání a nikoli pracovník podatelny, ačkoli v ostatních případech při jednoznačné identifikaci odesilatele tak může běžně činit.

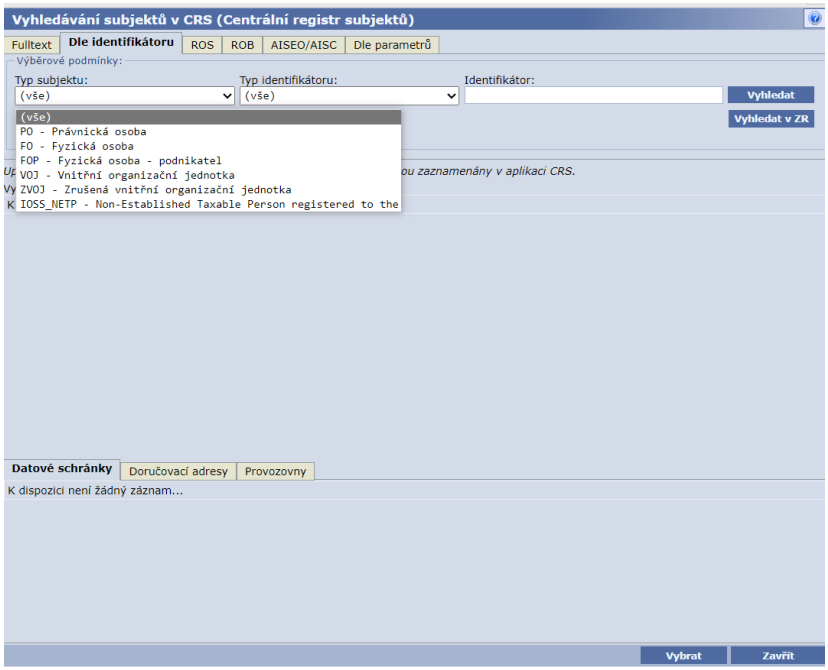
Novinkou v NSESSL a následně v atestačním řízení ve vztahu k jmennému rejstříku je rovněž požadavek na vytváření transakčních protokolů jmenného rejstříku. Jak již bylo zmíněno výše, Celní správa ČR je bezpečnostním sborem, který mimo jiné vykonává pátrací činnost, resp. trestní řízení. V takových případech není v zájmu bezpečnosti možné generovat transakční protokoly jmenného rejstříku s dotazy do Základních registrů. Došlo by tak k vážnému porušení bezpečnosti.

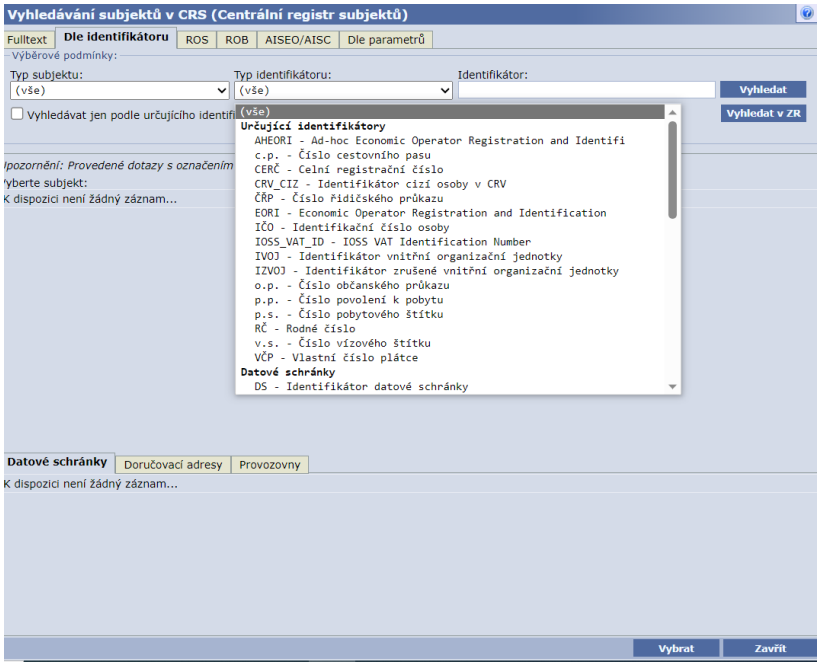
Obrázek 8 První krok při práci se jmenným rejstříkem – vyplnění obsahu

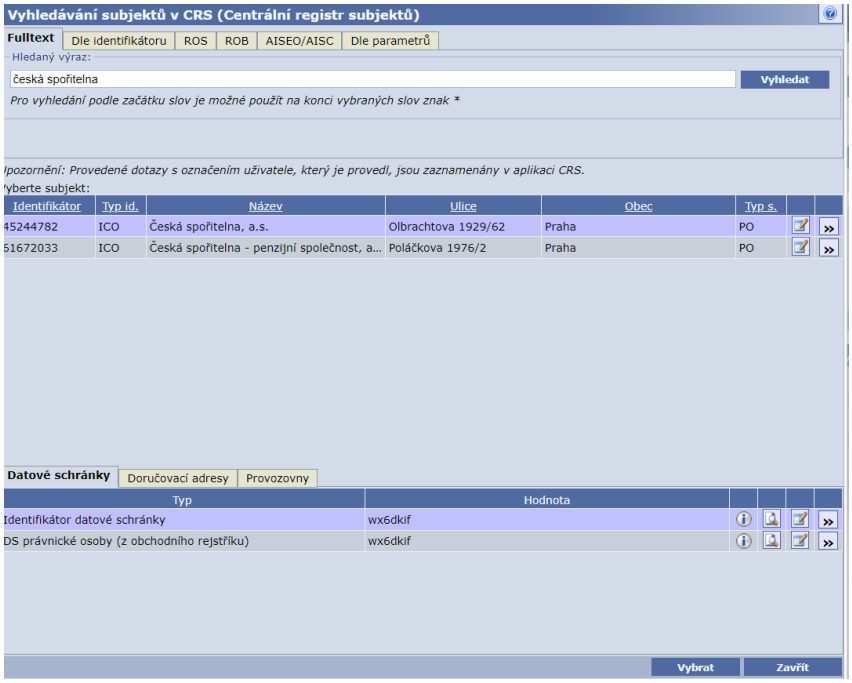


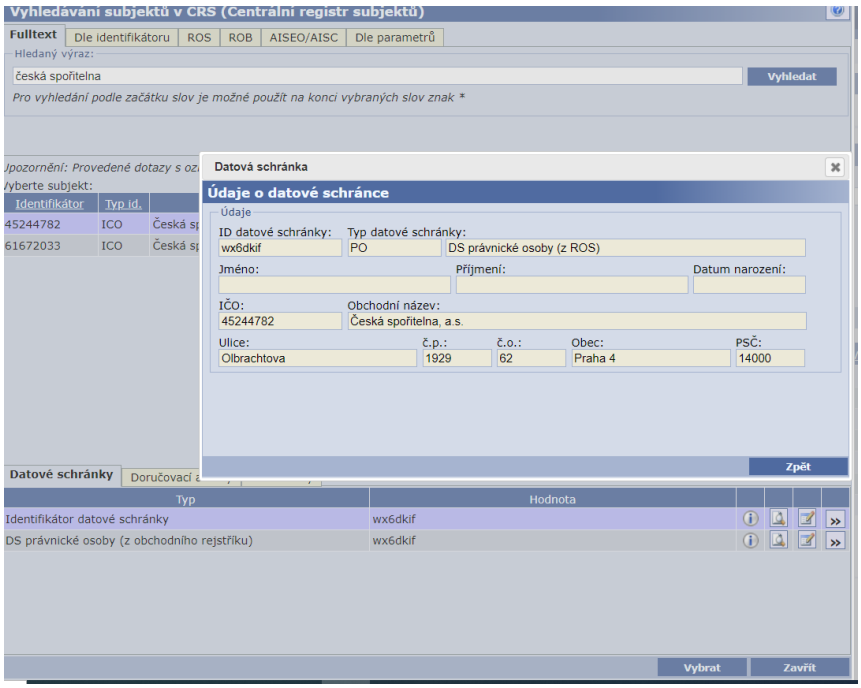
Zdroj: Celní správa ČR, eSAT (2023)

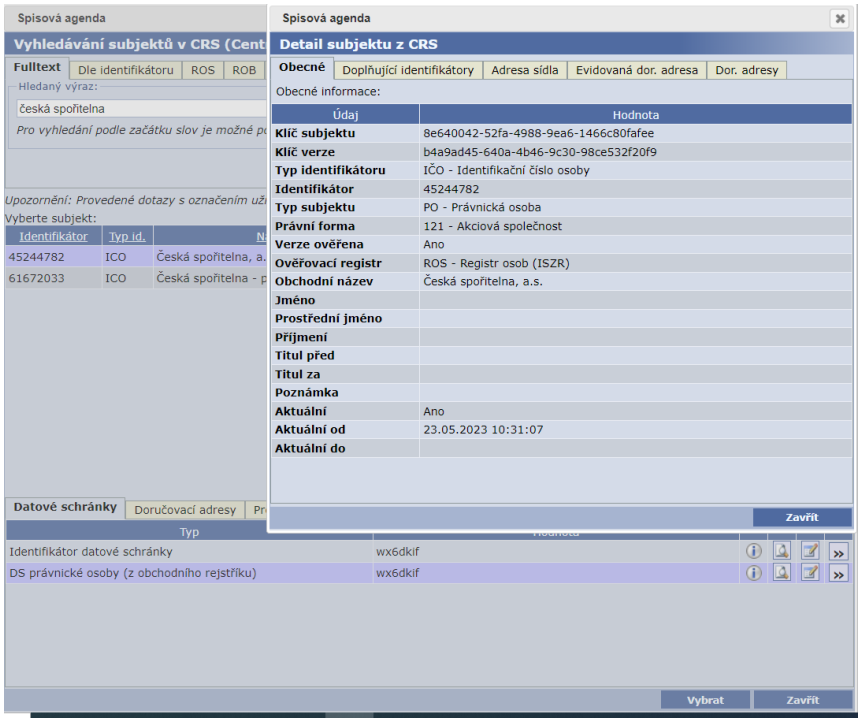
Obrázek 9 Vyhledání subjektu ve jmenném rejstříku dle identifikátorů

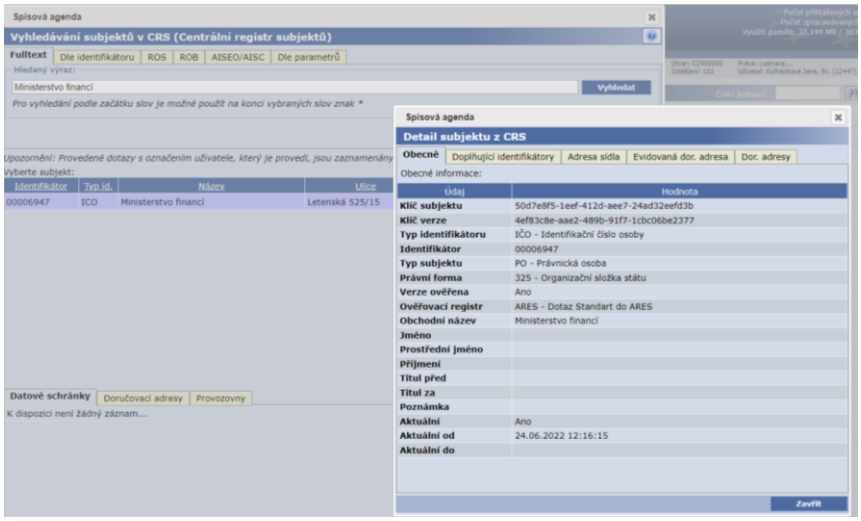


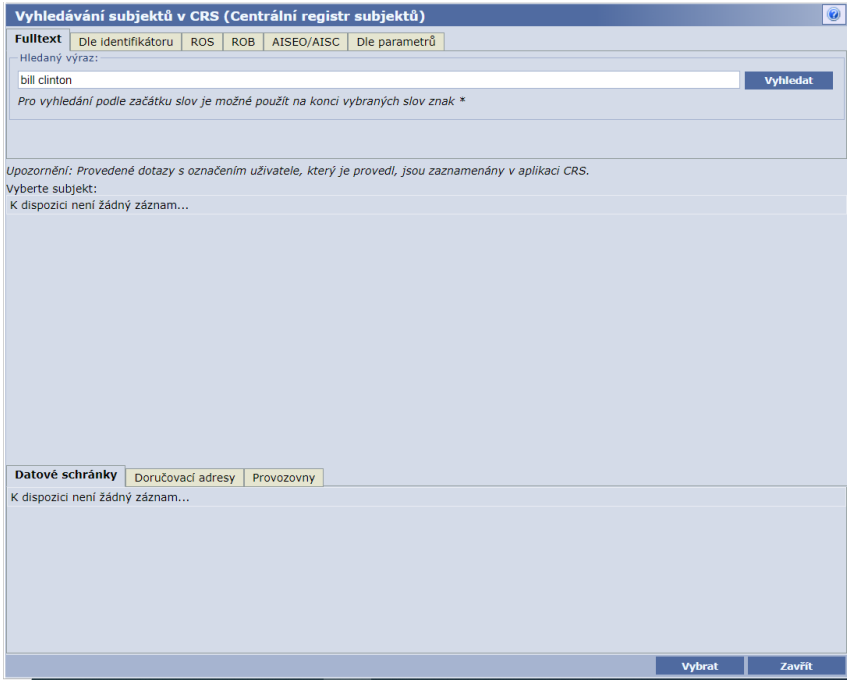



Vyhledávání subjektů v CRS (Centrální registr subjektů)
Fulltext
Dle identifikátoru
ROS
ROB
AISEO/AISC
Dle parametrů
Hledaný výraz:
česká spořitelna
Vyhledat
Pro vyhledání podle začátku slov je možné použít na konci vybraných slov znak *
Identifikátor
Typ id.
Název
Ulice
Obec
Typ s.
45244782
ICO
Česká spořitelna, a.s.
Olbrachtova 1929/62
Praha
PO
61672033
ICO
Česká spořitelna - penzijní společnost, a...
Poláčkova 1976/2
Praha
PO
Datové schránky
Doručovací adresy
Provozovny
Typ
Hodnota
Identifikátor datové schránky
wx6dkif
DS právnické osoby (z obchodního rejstříku)
wx6dkif
Vybrat
Zavřít


Vyhledávání subjektů v CRS (Centrální registr subjektů)
Fulltext
Dle identifikátoru
ROS
ROB
AISEO/AISC
Dle parametrů
Hledaný výraz:
česká spořitelna
Vyhledat
Pro vyhledání podle začátku slov je možné použít na konci vybraných slov znak *
Datová schránka
Údaje o datové schránce
Údaje
ID datové schránky:
wx6dkif
Typ datové schránky:
PO
DS právnické osoby (z ROS)
Jméno:
Příjmení:
Datum narození:
IČO:
45244782
Obchodní název:
Česká spořitelna, a.s.
Ulice:
Olbrachtova
č.p.:
1929
č.o.:
62
Obec:
Praha 4
PSČ:
14000
Zpět
Datové schránky
Typ
Hodnota
Identifikátor datové schránky
wx6dkif
DS právnické osoby (z obchodního rejstříku)
wx6dkif
Vybrat
Zavřít


Spisová agenda
Vyhledávání subjektů v CRS (Cent
Fulltext
Dle identifikátoru
ROS
ROB
Hledaný výraz:
česká spořitelna
Pro vyhledání podle začátku slov je možné p
Upozornění: Provedené dotazy s označením už
Vyberte subjekt:
Identifikátor
Typ id.
45244782
ICO
Česká spořitelna, a.
61672033
ICO
Česká spořitelna - p
Spisová agenda
Detail subjektu z CRS
Obecné
Doplňující identifikátory
Adresa sídla
Evidovaná dor. adresa
Dor. adresy
Obecné informace:
Údaj
Hodnota
Klíč subjektu
8e640042-52fa-4988-9ea6-1466c80fafee
Klíč verze
b4a9ad45-640a-4b46-9c30-98ce532f20f9
Typ identifikátoru
IČO - Identifikační číslo osoby
Identifikátor
45244782
Typ subjektu
PO - Právnická osoba
Právní forma
121 - Akciová společnost
Verze ověřena
Ano
Ověřovací registr
ROS - Registr osob (ISZR)
Obchodní název
Česká spořitelna, a.s.
Jméno
Prostřední jméno
Příjmení
Titul před
Titul za
Poznámka
Aktuální
Ano
Aktuální od
23.05.2023 10:31:07
Aktuální do
Zavřít
Datové schránky
Doručovací adresy
Typ
Identifikátor datové schránky
wx6dkif
DS právnické osoby (z obchodního rejstříku)
wx6dkif
Vybrat
Zavřít


Spisová agenda
Vyhledávání subjektů v CRS (Centrální registr subjektů)
Fulltext
Dle identifikátoru
ROS
ROB
AISEO/AISC
Dle parametrů
Hledaný výraz:
Ministerstvo financí
Vyhledat
Pro vyhledání podle začátku slov je možné použít na konci vybraných slov znak *
Upozornění: Provedené dotazy s označením uživatele, který je provedl, jsou zaznamenány
Vyberte subjekt:
Identifikátor
Typ id.
Název
Ulice
00006947
ICO
Ministerstvo financí
Letenská 525/15
Datové schránky
Doručovací adresy
Provozovny
K dispozici není žádný záznam...
Spisová agenda
Detail subjektu z CRS
Obecné
Doplňující identifikátory
Adresa sídla
Evidovaná dor. adresa
Dor. adresy
Obecné informace:
Údaj
Hodnota
Klíč subjektu
50d7e8f5-1eef-412d-aee7-24ad32eefd3b
Klíč verze
4ef83c8e-aae2-489b-91f7-1cbc06be2377
Typ identifikátoru
IČO - Identifikační číslo osoby
Identifikátor
00006947
Typ subjektu
PO - Právnická osoba
Právní forma
325 - Organizační složka státu
Verze ověřena
Ano
Ověřovací registr
ARES - Dotaz Standart do ARES
Obchodní název
Ministerstvo financí
Jméno
Prostřední jméno
Příjmení
Titul před
Titul za
Poznámka
Aktuální
Ano
Aktuální od
24.06.2022 12:16:15
Aktuální do
Zavřít



Zdroj: Celní správa ČR, eSAT (2003)

4.2.3 Zhodnocení vybraných aspektů životního cyklu dokumentu v Celní správě ČR

Výstupní datový formát zpracovávaných dokumentů

Výstupní datový formát zpracovávaných dokumentů je velké téma, které má ale své opodstatnění. Úvaha nad přijímanými formáty je proto více jak účelná. Ačkoli není snadné držet krok s neustále se rozvíjejícím technologickým vývojem, je třeba se novým formátům

i v eSSL přizpůsobovat a pracovat s nimi, což se Celní správě ČR daří. Příkladem může být i připravované multipodání či příjem formátu .zip.

Multipodáním je nazýváno takové podání, v kterém je možno zaevidovat další dokumenty k již zaevidovaným datovým a e-mailovým zprávám. V praxi se jedná např. o podání, kdy některé přílohy příchozí zprávy představují samostatná podání. V takovém případě je možné zaevidovat příchozí datové a e-mailové zprávy jako více čísel jednacích.

Při užití funkcionality multipodání se připravují dva možné způsoby evidování dokumentů a příloh příchozí zprávy, které mají být k dokumentům připojeny. Pokud je vybrána možnost „Jeden dokument“, je zaevidován jeden další dokument k datové zprávě a k němu jsou připojeny všechny vybrané přílohy. Pokud je vybrána volba „Hromadné zaevidování“, je pro každou vybranou přílohu zaevidován jeden dokument. Ke každému zaevidovanému dokumentu je připojena jedna příloha z příchozí zprávy. Samozřejmě že budou nabízeny pouze přílohy ve výstupním formátu nebo přílohy, u kterých je možné provést převod do výstupního datového formátu. Přílohy v jiných než výstupních formátech jsou automaticky převedeny do PDF.

V Celní správě ČR se rovněž testuje příjem formátu .zip, resp. příjem a automatické rozbalení .zip archivů při příjmu datových a e-mailových zpráv. V případě e-mailových zpráv je prováděna obsahová kontrola .zip archivů dle konfigurace aplikace (maximální počet souborů, povolené formáty a maximální počet úrovní adresářové struktury v .zip archivech). Zip archivy, které nesplňují konfigurované podmínky, nejsou zpracovány. Automatický převod do formátu PDF u nevýstupních formátů je prováděn i u souborů načtených ze .zip archivů.

Kontrola podpisu v rámci schvalovacího procesu

Kontrola elektronického podepisování je v rámci Celní správy ČR řešena jak po stránce technické (kvalifikovaný podpis na čipové zaměstnanecké kartě, časové razítko, kvalifikovaná pečeť, omezení v aplikaci eSAT), tak po stránce metodické. Podepisováním dokumentů jsou zpravidla pověřeni ředitelé nebo zaměstnanci k tomu pověření v souladu s příslušným vnitřním aktem řízení. Digitální dokumenty jsou podepisovány za pomoci automatizované podpory eSAT, který mimo jiné umožňuje, aby byl dokument před konečným schválením a podpisem akceptován více služebními funkcionáři v rámci jednoho nebo více útvarů. Podepisování v rámci samostatných evidencí dokumentů je opatřeno rovněž příslušnými vnitřními akty řízení.

Strojově čitelná vrstva

V případě velkého veřejnoprávního původce je takřka nemožné zajistit kontrolu každé komponenty tak, aby i pro zaměstnance existoval jednoduchý návod na správné vložení komponenty. Výkon spisové služby je pak paralyzován až na hranici nefunkčnosti. A naopak proklamovaný přínos pro osoby se zdravotním postižením je mizivý, neboť v Celní správě ČR případ takového nahlížení do spisu prozatím nebyl vůbec zaznamenán. Strojově čitelná vrstva má větší opodstatnění například v registru smluv, kde je předpoklad strojového využití podstatně větší než u dokumentů veřejnoprávního původce.

Jmenný rejstřík

Jmenný rejstřík je vhodným a užitečným nástrojem. Jeho využití např. v kombinaci s cPortálem je nesporné, díky čemuž je subjektům nabízena služba s velkým benefitem. Jak již bylo zmíněno výše, ač jsou kladeny na referenty Celní správy ČR větší požadavky ve smyslu ztotožňování, aplikačně se Celní správa ČR s celým tématem vypořádala více jak dobře, i když musela vyřešit systém ztotožňování fyzických a právnických osob neuvedených v Základních registrech (např. cizích státních příslušníků mimo Evropskou unii). Je nutné konstatovat, že i toto se jí podařilo. Důkazem je možnost vytvoření dokumentu s číslem jednacím při namátkových silničních kontrolách u zahraničních dopravců, kteří nejsou členy Evropské unie.

Další novinkou v NSESSL a následně požadavku v atestačním řízení ve vztahu k jmennému rejstříku je požadavek na vytváření transakčních protokolů. Tento požadavek se jeví jako nadbytečný, protože transakční protokoly jsou povinné již pro spisovou službu. Při vytváření transakčního protokolu ve jmenném rejstříku by zde musely být zaznamenány údaje i o subjektech, které má Celní správa ČR v šetření či sledování. Jedná se o informace v utajeném režimu, které nejsou přístupné veřejnosti. Došlo by tak k vážnému porušení bezpečnostních pravidel.

4.3 Chystaná atestace eSSL CS

4.3.1 Atestace elektronických systémů spisové služby

Atestace elektronických systémů spisové služby (dále jen „atestace eSSL“) je povinnost stanovena ZASS. Atestace eSSL je dle ZASS systémem ověření elektronického systému spisové služby dle požadavků ZASS, vyhlášky č. 259/2012 Sb. a příslušného NSESSL. Není možné a proveditelné, aby atest reflektoval další požadavky právního řádu,

jako je např. daňový či trestní řád. Atestace eSSL tedy potvrzuje jen a pouze soulad s výše uvedenými předpisy.

Atestace eSSL se nezabývají správným používáním eSSL u jednotlivých veřejnoprávních původců. Během atestace musí dodavatel prokázat, že jeho používaný eSSL splňuje požadavky, resp. všechny požadavky uvedené ve třech výše jmenovaných právních předpisech, které jsou seskupeny do tzv. atestačních scénářů.

Mechanismus atestací byl zavedený zákonem DEPO. Původní termín spuštění atestací eSSL byl stanoven na únor 2022. Nicméně se tak nestalo z důvodu požadavků odborné veřejnosti na důkladnější pojetí atestací, než jaké bylo nastíněno a připraveno Ministerstvem vnitra ČR. Z toho důvodu došlo k odložení a důkladnějšímu propracování atestačních požadavků. Z důvodu složitosti a náročnosti atestací eSSL, a to jak po stránce technické, tak odborné, došlo Ministerstva vnitra ČR s Českou agenturou pro standardizaci. Zákon sice svěřuje atestační kompetence Ministerstvu vnitra ČR, tzn. MV ČR může být samo atestačním střediskem, ale zároveň také může pověřit atestační činností subjekt jiný, a to dle určitých podmínek:

- jedná-li se o subjekt v majetku státu;
- zvolený subjekt nesmí být ve střetu zájmů;
- zvolený subjekt musí disponovat patřičnou odborností.

Na základě těchto podmínek byla Ministerstvem vnitra ČR pověřena atestační činností Česká agentura pro standardizaci (dále „ČAS“). Tato agentura byla založena dne 1. ledna 2018 jako státní příspěvková organizace Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví dle zákona č. 265/2017 Sb. Do gesce ČAS spadají všechny činnosti související s technickými normami, a to včetně jejich vytváření, vydávání a distribuce. Na NSESSL je možno pohlížet do jisté míry jako na druh technické normy. Z toho důvodu byl ČAS vybrán pro spolupráci na atestacích eSSL, protože právě on má mít s atestacemi největší zkušenosti.

Koho se atestace eSSL týká

Atestace eSSL se týkají elektronických systémů spisových služeb veřejnoprávních původců (organizační složky státu, ozbrojené a bezpečnostní složky, územní samosprávné celky včetně jejich organizačních složek, státní příspěvkové organizace, státní podniky, zdravotní pojišťovny, školy atd.), nikoli soukromých subjektů (tzn. soukromý sektor). Jedná

se tedy o povinnost veřejnoprávního původce splňovat požadavky na eSSL uvedené v NSESSL tak, aby byly dodrženy.

Povinnost atestací eSSL dopadá jak na veřejnoprávní původce, kteří musí plnit zákonnou povinnost používat od 1. ledna 2026 atestovanou eSSL, tak rovněž i na poskytovatele/dodavatele/výrobce eSSL, tzn. výrobce spisových služeb, kteří nesmějí od 1. července 2024, resp. od 1. ledna 2025 nabízet neatestovaný eSSL. eSSL bude moci nabízet takový dodavatel spisové služby, kterému byl udělen atest atestačním střediskem ČAS.

ESSL, které nebudou vlastnit platný atest od ČAS, se vystavují riziku porušení zákona a udělení pokuty. Zákon jasně zakazuje používání neatestované eSSL. Sankce jsou v takovém případě následující:

- 200 tis. Kč za používání neatestované eSSL pro veřejnoprávní původce;
- 1 mil. Kč za nabízení neatestované eSSL.

Ačkoli by se mohlo zdát, že zaplatit pokutu bude levnější než podstupovat případný celý proces výměny dodavatele či přímo získání atestace, je třeba upozornit na fakt, že by se při takovém postupu jednalo o správní delikt.

Základní informace k atestacím eSSL

O atest eSSL může požádat prakticky kdokoli – poskytovatel eSSL, veřejnoprávní původce, distributor eSSL. ZASS nijak nestanovuje subjekt žádající o atestace eSSL. Zákon pouze stanovuje, že za atestaci hradí objednavatel atestace Atestačnímu středisku úplatu. Nicméně v kombinaci s ust. 69e ZASS, které zakazuje nabízet veřejnoprávnímu původci neatestovanou eSSL, je jasné, že to budou dodavatelé.

Atestace je prováděna na základě objednávky, atestační úkon je zpoplatněn. Cena atestace eSSL je aktuálně fixně stanovena částkou 489 000,- Kč bez DPH. Platba má být hrazena zálohovou fakturou České agentuře pro standardizaci, a to do 14 dnů po objednání atestace, resp. po zaslání zálohové faktury objednavateli atestace. Atestační středisko má zákonem stanovenu dobu, za kterou musí atestační proces provést, a to 3 měsíce od zaplacení zálohové faktury objednavatelem.

<u>Doba platnosti udělené atestace eSSL</u>

V modelovém případě je doba platnosti udělené atestace eSSL 2 roky. Po dvou letech atestace exspiruje a subjekt musí žádat o atestaci eSSL znovu. Atestační proces se tak bude

opakovat každé dva roky, díky čemuž má dojít k zajištění akceptace všech zákonných požadavků do eSSL ve shodě se ZASS, vyhláškou i NSESSL.

Verzování eSSL

Poskytovatel eSSL může prodávat či používat pouze verze eSSL, kterým byl udělen Atestačním střediskem ČAS atest. Udělení atestu ovšem není vyžadováno při vylepšení eSSL ze strany uživatelské přívětivosti, změně v kyber bezpečnostních parametrech atd. To znamená, že upgrade nebo nová verze eSSL je možná za předpokladu (a prohlášení poskytovatele), že nedošlo ke změnám v atestovaných parametrech. Pokud došlo v atestované verzi eSSL ke změně ve vztahu k atestačním scénářům, atestace eSSL ztrácí platnost a na eSSL je pohlíženo jako na eSSL bez atestu.

Jak je z výše uvedeného patrné, atestován bude systém, nikoli výrobce. Samozřejmě že platí, že výrobce může mít v portfoliu více atestovaných eSSL. Příkladem může být klasická a cloudová eSSL.

Ukončování atestací v případě legislativních změn

V tomto bodě se musí poskytovatel eSSL maximálně spolehnout na Ministerstvo vnitra ČR a doufat, že nedojde k vydání novelizace ZASS, vyhlášky nebo NSESSL, který by svým obsahem zasáhl do povinnosti atestací. Takovým zásahem by došlo k tomu, že udělené atestace eSSL pozbývají platnosti. Platnost atestu pak nekončí po 2 letech, ale nejvýše po 1 roce od platnosti nové legislativní změny. Jestliže má sama atestace platnost pouze dva roky, zkrácení platnosti atestace při legislativní změně na jeden rok ztrácí ze své podstaty význam. Zkrácení platnosti atestační doby by se jevila jako opodstatněná při např. pětileté či víceleté platnosti atestace.

Na druhou stranu by se dalo očekávat, že pod tlakem nových atestací dojde i ze strany Ministerstva vnitra ČR k větší koncepčnosti ve směru k vydávání legislativních změn. Tyto úvahy poukazují na fakt, že současná novela vyhlášky a NSESS bude vbrzku opět novelizována. Ve světě eSSL se nastavují nová pravidla a implementují se do systémů eSSL nové požadavky za velké finanční částky, aniž by byly všechny podmínky a postupy na začátku jasně stanoveny.

Atestace a poskytovatelé eSSL

Vzhledem k povinnosti nabízet veřejnoprávním subjektům od 1. ledna 2026 pouze atestované systémy eSSL, je možno rozdělit poskytovatele eSSL do dvou, resp. tří skupin.

První skupina podstoupí atestační proces a bude nabízet svůj atestovaný produkt veřejnoprávním původcům. Do této skupiny budou dozajista spadat nejvýznamnější firmy na trhu s eSSL, mezi které patří např. GORDIC spol. s r.o., ICZ a.s. a Triada, spol. s r. o. U těchto společností je možno očekávat velký rozvoj, protože po získání atestu budou moci začít okamžitě nabízet atestované eSSL veřejnoprávním subjektům, které teprve s eSSL budou začínat (např. školy). Rovněž tak mohou obsadit místa dodavatelů eSSL, kteří se atestů buď nebudou účastnit či atest nezískají. Prognózou je, že trh s eSSL u veřejnoprávních původců bude zeštíhlen a rozdělen mezi několik málo dominantních společností, které mají finanční prostředky na dopracování systémů eSSL dle nových požadavků. Je třeba si uvědomit, že se jedná o mnohamilionové částky, které budou muset poskytovatelé zainvestovat do eSSL pro dotvoření všech požadavků nutných pro získání atestace. Lze předpokládat, že celkové náklady poskytovatelů eSSL budou následně rozmělněny do cen účtovaných jednotlivým veřejnoprávním původcům, kteří si jejich produkt zvolí. Náklady na eSSL pro tyto veřejnoprávní původce budou sice vyšší, nikoli ovšem enormně.

Druhou skupinou jsou drobnější poskytovatelé eSSL, kteří nebudou moci či schopni získat atest pro své eSSL. Důvodem mohou být velice vysoké finanční náklady na rozšíření eSSL dle požadavků ČAS. Takové společnosti tak nebudou moci poskytovat eSSL veřejnoprávním původcům, což je buď donutí trh opustit, nebo se zaměřit na ostatní subjekty (soukromé subjekty, firmy). Další variantou může být i ukončení jejich činnosti. V takovém případě je možné říct, že nutnost atestací je pro menší subjekty devastační.

Třetí skupinou „provozovatelů“ eSSL jsou ti veřejnoprávní původci, kteří si v průběhu doby vytvořili své vlastní eSSL, ať vlastními silami nebo za pomoci dodavatelských společností. Často se jedná o modulární řešení eSSL, což je eSSL sestavená z několika částí modulů dodávaných rozdílnými dodavateli. Jedná se tak o eSSL vytvořený na míru veřejnoprávního původce, která reflektuje jeho individuální potřeby. Vybudovali tak jedinečný eSSL systém, který plně odpovídá jejich potřebám, reflektuje na jejich specifické požadavky a přizpůsobuje se prostředí informačních systémů daného původce. Je nutné podotknout, že takto zbudovaný systém musí plně odpovídat zákonným požadavkům kladených na eSSL veřejnoprávních původců.

Co znamená atestace eSSL

Jedná se o zhodnocení implementace požadavků ZASS, vyhlášky a NSESSL na eSSL do jednotlivých nabízených či používaných eSSL, a to ve smyslu: splnil-nesplnil či

obsahuje-neobsahuje daný produkt určitý požadavek. Atestace eSSL se týkají software. Atestace eSSL se netýkají správnosti pracovních postupů uživatelů v daném eSSL. Dozor nad výkonem spisové služby spadá do gesce Národního archivu a odboru Archivní správy Ministerstva vnitra ČR.

Atestace eSSL – atestační scénáře

Položek k implementaci do eSSL uvedených v NSESSL ve vztahu ke spisové službě je přibližně 300. ČAS všechny zákonné položky vyselektoval a sloučil do skupin. Na základě atestačních požadavků byly vytvořeny typové situace, tzv. atestační scénáře. Testovací scénáře na sebe navazují tam, kde je to možné, proto je třeba dodržovat jejich posloupnost. Důvodem je jejich práce s entitami vytvořenými v předchozích scénářích (např. nejprve je třeba ověřit správnost přijetí dokumentu a v dalším testovacím scénáři jeho zařazení do spisu), proto není možné měnit pořadí testovacích scénářů.

Nyní je publikováno 33 atestačních scénářů a další 3 atestační scénáře se připravují. Každý scénář obsahuje daný počet požadavků (maximum: atestační scénář TS12 – 32 požadavků). Atestovaný eSSL musí projít zdárně všemi scénáři. Pro udělení platného atestu musí být úspěšnost 100 %.

4.3.2 Postup veřejnoprávního původce při získání atestu eSSL

Před objednáním atestačního procesu je třeba podstoupit několik doporučených kroků, které mají usnadnit poskytovateli eSSL získání atestu eSSL. Jedná se o analýzu a přípravu na nečisto. Tyto kroky je potřebné učinit, protože ačkoli termín atestací eSSL byl odložen z 1. ledna 2025 na 1. ledna 2026, jedná se i tak v prostředí veřejné správy o vcelku hraniční termín.

Analýza

Prvním doporučeným krokem pro získání atestace eSSL je analýza eSSL daného veřejnoprávního původce. Je třeba analyzovat smluvní vztahy mezi dodavatelem a příjemcem eSSL, včetně jejich další spolupráce do budoucna. Rovněž je nezbytné podrobit analýze celý eSSL a zhodnotit současný stav dané eSSL ve vztahu k atestačním scénářům. Na základě toho se musí veřejnoprávní původce rozhodnout, jak bude pokračovat dále. V této etapě je ještě prostor na oslovení nového dodavatele eSSL a vypsání veřejné zakázky na nového poskytovatele eSSL, případně na změnu technických parametrů stávajících smluv. Pokud se rozhodne veřejnoprávní původce setrvat v současných smluvních

podmínkách, tzn. nebude měnit dodavatele eSSL, musí začít do eSSL zapracovávat nové zákonné požadavky do eSSL ve shodě s atestačním scénáři.

Atestace nanečisto

Na atestaci je možno eSSL připravit díky publikovaným atestačním scénářům, které jsou volně dostupné na webových stránkách České agentury pro standardizaci. ČAS garantuje atestační postup dle těchto publikovaných atestačních scénářů. Vyzkoušení atestace nanečisto v „domácím prostředí“ se proto jeví jako logický a zároveň nutný krok, díky němuž bude žadatel o atestaci schopen identifikovat případné nedostatky eSSL a následně je odstranit.

Při testování v domácím prostředí by měly rovněž vzniknout návody práce s daným systémem eSSL pro testery ČAS. Formát návodů není přesně stanoven. Může se jednat o videonahrávku, návod sestavený z printscreenů či písemný návod. Forma je na žadateli o atestaci.

Příprava eSSL k atestaci

Jedná se o krok, během něhož bude nahrána/nainstalována spisová služba do virtuálního prostředí ČAS. Jedná se o poslední okamžik, kdy veřejnoprávní původce či poskytovatel eSSL bude mít přístup do poskytovaného eSSL. Časová dotace na nahrání eSSL do prostředí ČAS je v řádu několika dnů.

Atestace se budou provádět ve třech možných prostředích, a to:

- ve virtuálním hardwarovém prostředí atestačního střediska ČAS;
- ve vlastním hardware objednavatele, které je také v prostředí objednavatele – volba tohoto prostředí je třeba zdůvodnit v atestační žádosti a prokázat tak, že objednavatel nemůže využít virtuálního hardwarového prostředí atestačního střediska ČAS. V takovém případě musí objednavatel umožnit testerům práci v daném prostředí a to tak, aby on sám do prostředí během testování neměl přístup;
- v cloudovém prostředí, které rovněž zajistí objednavatel – tato varianta je možná v případě, je-li v katalogu cloud computingu pro orgány veřejné správy podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

První způsob testování s využitím laboratorního prostředí ČAS bude pravděpodobně nejvyužívanější.

Vlastní testování

Vlastní testování bude probíhat pouze v režii ČAS, a to dle testovacích scénářů publikovaných na webových stránkách ČAS. Žadatel o atest musí zpracovat kompletní dokumentaci, kterou předloží s požadavkem k atestaci. Testovat budou testeři ČAS, a to dle dodaných návodů. Cílem bude prokázat, zda daný software či aplikace splňuje každý požadavek ZASS, vyhlášky a NSESSL. Znamená to, že daný eSSL musí obsahovat všechny varianty požadavků uvedených v ZASS, vyhlášce a NSESSL, a to i ty, které jsou ve výše uvedených dokumentech ve variantním řešení (buď-nebo).

Vyhodnocení atestace

Ve finální části dojde k vyhodnocení atestačního procesu. Jestliže eSSL splní na 100 % všechny atestační scénáře, bude mu udělena atestace. Systém eSSL bude prohlášen za shodný dle požadavků ZASS, vyhlášky a NSESSL. Nebude-li atest udělen, může následovat odvolání a přezkum. Atestační proces může být ukončen udělením atestu nebo zamítnutím udělení atestu, tzn. ukončením atestace bez vydání atestačního ověření.

4.3.3 Atestace ve vztahu k eSSL Celní správy ČR

Celní správa ČR bude muset stejně jako ostatní veřejnoprávní původci podstoupit proces atestací v ČAS.

Jak již bylo zmíněno výše, v případě Celní správy ČR se jedná o elektronický systém spisové služby, což znamená, že se bude atestovat systém aktivní a nadmíru složitý, postupně budovaný od roku 2008. Z popisu vykonávané činnosti Celní správou ČR je patrno, že se jedná o systém modulární, který se skládá z centrálního páteřního systému tvořeného spisovou službou eSAT. Na eSAT se postupem let navázaly agendové aplikace, samostatné evidence dokumentů, jmenný rejstřík, cPortál a také elektronická spisovna.

Rovněž téma bezpečnosti nesmí být opomíjeno. Celní správa ČR jako bezpečnostní sbor vykonává pátrací a sledovací činnost, tudíž se jedná o v rámci eSSL o činnost podléhající značným bezpečnostním opatřením.

V současné době v Celní správě ČR probíhá podrobná analýza eSSL. Přesto už teď je patrno, že rozvázat smluvní vztahy se současnými dodavateli jednotlivých segmentů eSSL a nahradit je odpovídajícími novými dodavateli s předpokládaným atestem eSSL, je zhola nemožné – časově i finančně.

V obdobné situaci není pouze Celní správa ČR, ale i ostatní veřejnoprávní původci. Je běžné, že eSSL řady veřejnoprávních původců je vykonávána ve více SW aplikacích. Vlivem právní úpravy veřejných zakázek často dochází k tomu, že aplikace jsou dodávány více dodavateli. Pak je vyloučené, aby žadatelem o atestaci byl dodavatel, neboť jeden z dodavatelů nemůže zaručit soulad takto vykonávané eSSL s požadavky atestačních scénářů jako celku. V tomto případě je jediným možným žadatelem o atestaci, včetně povinnosti uhradit úplatu, veřejnoprávní původce sám. Celní správa ČR bude muset pravděpodobně zažádat o atestace eSSL sama. Velikou výhodou v tomto případě je, že spisová služba a jmenný rejstřík jsou do Celní správy ČR dodávány jednou dodavatelskou firmou. Tento případ se ovšem netýká elektronické spisovny, jejímž dodavatelem se v řádné soutěži stala odlišná společnost.

4.3.4 Zhodnocení vybraných aspektů životního cyklu dokumentu v Celní správě ČR ve vztahu k atestacím NSESSL

Výstupní datový formát zpracovávaných dokumentů v atestacích NSESSL – požadavky na datové formáty uvedené v atestačních scénářích

Datové formáty se prolínají všemi testovacími scénáři. Zevrubně se jim věnuje atestační scénář číslo TS02 Konfigurace eSSL.

Kromě výstupních datových formátů má veřejnoprávní původce umožnit příjem dokumentů v digitální podobě, resp. digitálních dokumentů sestávající z komponent v datových formátech pro:

- statické textové dokumenty typu .doc, .xlsx, .ppt, .txt, .PDF, .htm, .html apod.;
- statické kombinované textové a obrazové dokumenty;
- statické obrazové dokumenty – PDF/a-3, zfo, .eml, zip apod.

V testovacím scénáři TS09a, který se věnuje příjmu dokumentů, je stanoven požadavek na výstupní datové formáty alespoň v datových formátech stanovených jako výstupní datové formáty, případně formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě.

V návaznosti na požadavky uvedené v testovacím scénáři TS02 je možné konstatovat, že Celní správa ČR splňuje požadavky tohoto scénáře beze zbytku. V současné době již testuje implementaci .zip formátu v datové zprávě. Zip formát bude automaticky rozbalován při příjmu datových a e-mailových zpráv. V případě e-mailových zpráv je prováděna obsahová kontrola zip archívů dle konfigurace aplikace (maximální počet souborů, povelné formáty a maximální počet úrovní adresářové struktury v zip archivech),

Zip archívy, které nebudou splňovat konfigurované podmínky, nebudou zpracovávány. V detailu příchozí datové nebo e-mailové zprávy jsou zip archivy a soubory načtené ze zip archivů pro odlišení znázorněny novými ikonami (obrázek 10).

Obrázek 10 Dialogové okno s detailem datové zprávy obsahující .zip formát

Zdroj: Celní správa ČR, eSAT (2023)

Kontrola podpisu v rámci schvalovacího procesu v atestacích NSESSL

V testovacím scénáři TS18c Vedení dokumentu je stanoven požadavek týkající se dokumentu pro odeslání, kdy bude simulován pokus o podepsání poškozené komponenty ve formátu .docx. V takovém případě má eSSL před podepsáním automaticky zajistit změnu datového formátu komponenty, a to do PDF/A. Tento formát musí být opatřen potřebnými metadaty ve formátu .xml (poznámka: metadatům je speciálně věnován testovací scénář

TS04a a TS04b). Dokument musí být následně opatřen elektronickým podpisem včetně kvalifikovaného elektronického časového razítka.

eSSL Celní správy ČR požadavky na elektronické podpisy, včetně kvalifikovaného časového razítka, dlouhodobě splňuje, neboť již v roce 2016 byly implementovány požadavky evropského nařízení eIDAS. Aplikace eSAT při podpisu dokumentu ve spisové službě nabízí pouze možnost kvalifikovaného elektronického podpisu. Přiložení kvalifikovaného elektronického časového razítka je standardním postupem, časové razítko je přikládáno ke všem dokumentům v eSAT.

Zajišťovacím prvkům se dále věnuje testovací scénář TS24 Zajišťovací prvky. Tyto scénáře leží ovšem mimo záběr této práce.

Strojově čitelná vrstva v atestacích NSESSL

Zajištění strojově čitelné vrstvy je stanoveno povinností podle § 16 vyhlášky 259/2012 Sb. V atestačních scénářích se tomuto bodu věnuje scénář TS18c Vedení dokumentu. Požadavek je v atestačním scénáři postaven tak, že pokud je vykonávána spisová služba v eSSL, musí být komponenta opatřena strojově čitelnou vrstvou, a to jak komponenta textová, tak i komponenta kombinovaná (textová a obrazová). V atestačních scénářích ovšem není brán zřetel na to, že komponenta se strojově nečitelnou vrstvou se může objevit i ve vlastním dokumentu veřejnoprávního původce – např. jako zkopírovaná příloha. Toto vymezení v podstatě vylučuje atestaci, což jen dotvrzuje komplikovanost a v podstatě i nadbytečnost této povinnosti.

Celní správa ČR se strojově čitelnou vrstvou pracuje. Bohužel je nutné konstatovat, že se setkává s řadou případů, kdy je velmi problematické, někdy nemožné, požadavek strojově čitelné vrstvy realizovat. Příkladem může být moment, kdy do vlastního čísla jednacího je nutné vložit dokumenty stažené z veřejně přístupného rejstříku (např. Obchodní rejstřík, Katastr nemovitostí), které ovšem textovou vrstvu samy neobsahují – viz výše.

Kvůli dodržení tohoto požadavku a problémům se správným vytvářením strojově čitelné vrstvy byla aplikace eSAT upravena tak, aby bylo vkládání textových dokumentů bez strojově čitelné vrstvy blokováno, takový textový dokument není možné do aplikace eSAT vložit.

Jmenný rejstřík v atestacích NSESSL

Jmennému rejstříku se věnuje atestační scénář TS01 Jmenný rejstřík. Atestační agentura bude během atestačního procesu testovat následující funkce jmenného rejstříku eSSL:

- dovednost přijímat notifikace z informačních systémů Základních registrů;
- automatickou kontrolu eSSL oproti základním registrům při odesílání a příjmu dokumentů;
- ztotožnění osob v záznamech jmenného rejstříku oproti Základním registrům a ISDS;
- transakční protokoly jmenného rejstříku.

Atestace budou ověřovat schopnost ztotožnění subjektů vůči Základním registrům. Tuto funkcionalitu má Celní správa ČR implementovánu do eSSL již od roku 2022 přes jmenný rejstřík v Základních registrech. Celní správa ČR dokáže výborně pracovat s údaji zahraničních subjektů, které v Základních registrech nejsou uvedeny.

Problém atestačního scénáře TS01 Jmenný rejstřík je v požadavku na zapisování veškerých operací se záznamy do transakčního protokolu jmenného rejstříku. V současnosti má transakční protokol eSSL zaznamenávat veškeré operace prováděné ve jmenném rejstříku, a to hlavně vytváření, úpravy, zničení a nahlížení na záznamy.

Tento požadavek by se zdál oprávněn u běžného veřejnoprávního původce, nikoli ovšem v rámci původce, kterým je bezpečnostní sbor. Celní správa ČR vykonává rovněž pátrací a sledovací činnost, v návaznosti je na veškeré záznamy v transakčním protokolu jmenného rejstříku pohlíženo jako na prolomení bezpečnostních opatření.

Jmenný rejstřík musí být součástí každého systému elektronické spisové služby jako celku (byť v samostatné SW aplikaci), a proto se i na něj vztahují atestace. Jmenný rejstřík je součástí testovacích scénářů, čímž by měl být prokázán jeho soulad se zákonem, vyhláškou a NSESSL.

Na příkladu Celní správy ČR je možno prezentovat nedopracovanost atestačních požadavků, resp. nereflektování skutečného stavu výstavby architektury systémů pro správu dokumentů. Veřejnoprávní původci měli při řešení implementace volnou ruku, a tudíž ji vyřešili různým způsobem, resp. od různých dodavatelů. Zejména vedení jmenného rejstříku bývá řešeno mimo základní spisovou službu – a to proto, aby údaje mohly volně nabírat samostatné evidence dokumentů. Toto řešení bylo dokonce v minulosti odborem Archivní správy Ministerstva vnitra ČR doporučováno. Klíčovou otázkou se stalo, kdo je

poskytovatelem jmenného rejstříku u daného veřejnoprávního původce, resp. jestli se jedná o shodného poskytovatele i pro spisovou službu. Výhodou pro Celní správy ČR je, že dodavatel spisové služby eSAT a Centrálního registru subjektů, je shodný. Řadu veřejnoprávních poskytovatelů však čeká další investice do rozvoje, kdy se budou muset rozhodnout, zda implementují jmenný rejstřík do eSSL, anebo jej ponechají mimo, a tudíž se stanou objednavatelem a plátcem atestace.

5 Výsledky a diskuse

Autorka se v diplomové práci zabývá analýzou informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby jako páteřního systému u veřejnoprávních původců. Na příkladu Celní správy České republiky ukazuje složitost elektronického systému spisové služby.

Analyzuje novelizace stěžejních legislativních předpisů (zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů – ZASS, vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů a Národní standard pro elektronické systémy spisové služby) a zavedení povinných atestací dle Národního standardu pro elektronické systémy spisové služby – NSESSL.

Autorka poukazuje na to, že atestace eSSL se staly nezbytnou podmínkou spisové služby a očekává zvýšení kvality poskytovaného produktu na trhu, tzn. poskytovaných eSSL. Je ovšem nutné, aby atestační pravidla byla nastavena jednoznačně, co do výkladu srozumitelně a nezpochybnitelně. Na atestační požadavky, díky již probíhajícím aktualizacím atestačních scénářů, nelze dle autorky bohužel pohlížet jinak, než jako na uspěchané a nepřipravené. Rovněž predikuje nutnost úpravy současných platných atestačních scénářů, díky čemuž nutně musí dojít také k oddálení termínu povinných atestací eSSL.

Tvrzení, že bylo nutné měnit vyhlášku a NSESSL kvůli atestacím, je liché, protože v době přijetí zákona DEPO byla účinná jak vyhláška, tak NSESSL a nebyl problém atestovat dle tehdejšího právního stavu. Základní otázkou je, zda je nutné na eSSL veřejnoprávního původce klást tak enormní množství požadavků, což koneckonců nyní opatrně připouští i ministerstvo vnitra (viz semináře k atestacím eSSL konané NA ČR a ČAS), které se zabývá myšlenkou zavést pro některé typy původců zjednodušenou spisovou službu.

Autorka se věnuje čtyřem tématům ve vztahu ke spisové službě, a to výstupnímu datovému formátu zpracovávaných dokumentů, strojově čitelné vrstvě, kontrole podpisu v rámci schvalovacího procesu a ztotožnění subjektu ve jmenném rejstříku. Na zvolených příkladech ukazuje, jak jsou řešeny u konkrétního veřejnoprávního původce a uvádí příklady, kdy jsou požadavky vycházející z NSESSL z pozice veřejnoprávního původce nadbytečné. Na příkladu Celní správy ČR je patrné, že veřejnoprávní původci stanovené požadavky na eSSL ve shodě se ZASS, vyhláškou a NSESSL běžně do eSSL zapracovávají.

Jako problémovým se jednoznačně jeví požadavek na zajištění strojově čitelné vrstvy, kterou mají být opatřeny všechny dokumenty a jejich komponenty u veřejnoprávního původce. V NSESSL ovšem není brán zřetel na to, že komponenta se strojově nečitelnou vrstvou se může objevit i ve vlastním dokumentu veřejnoprávního původce – např. jako zkopírovaná příloha. Toto jen dotvrzuje komplikovanost a v podstatě i nadbytečnost této povinnosti. Autorka poukazuje na případy, kdy je velmi problematické, někdy nemožné, požadavek strojově čitelné vrstvy realizovat. Příkladem může být moment, kdy do vlastního čísla jednacího je nutné vložit dokumenty stažené z veřejně přístupného rejstříku (např. Obchodní rejstřík, Katastr nemovitostí), které ovšem textovou vrstvu samy neobsahují. Autorka požadavek strojově čitelné vrstvy hodnotí jako jednoznačně nadbytečný.

Zejména v návaznosti na NSESSL ovšem vyvstává v atestacích požadavek, aby eSSL obsahoval všechny požadavky uvedené ve výše zmiňované legislativě – tzn. i variantní řešení typu buď-nebo. Na tento požadavek je možno pohlížet jako na zásadní, protože nutí veřejnoprávní původce a výrobce eSSL zapracovat veškeré varianty řešení, i když je veřejnoprávní původce jako zákazník nevyžaduje a nepoužívá, čímž mimo jiné enormně vzroste robustnost eSSL, ale hlavně finanční náklady na eSSL, a to v řádu milionů Kč. Přitom stačí striktně dodržovat ZASS, vyhlášku a NSESSL po stránce technické stavby eSSL a držet se požadavků v ZASS, které jasně specifikují úkoly, které má eSSL splňovat. Na požadavek udržování všech variantních řešení lze jednoznačně pohlížet jako na nadbytečný.

Atestace eSSL jsou dle názoru autorky enormně drahé, a to jednak samotnou výší úplaty (489 000,- Kč), jednak člověko/hodinami na straně dodavatele i původce (viz např. představa o nahrávání video návodů objednavatelem služby atestačnímu středisku ČAS). Z náročnosti příprav eSSL na atestace eSSL je zřejmé, že značně vzroste odborná i finanční zátěž pro veřejnoprávního původce i dodavatele eSSL. Je třeba zdůraznit, že nebyla vyslyšena námitka původců, že jejich činnost spočívá v jiných úkolech, než je archivnictví a spisová služba.

Rovněž dvouletá platnost atestu je příliš krátká, což je pro dodavatele eSSL silně zatěžující. Jestliže nedojde k legislativním změnám, autorka nevidí opodstatnění v takto krátké platnosti atestace. V takovém případě bude dodavatel eSSL přecházet od jednoho atestačního řízení k dalšímu. Veřejnoprávního původce toto velice zatíží. Autorka je přesvědčena, že na základě provozních možností původce, dodavatele eSSL i aplikace samotné je optimální lhůtou pro platnost atestačního osvědčení pět let.

Autorka se na základě své praxe i zde provedené analýzy domnívá, že je třeba jednoznačně snížit a zjednodušit počet požadavků, které jsou z pozice NSESSL kontrolovány. Některé z požadavků (např. povinně daná podoba spisu bez návaznosti na procesní správní předpisy jako je např. daňový řád) jsou potřebné jen pro příslušný archiv v rámci skartačního řízení, přičemž neopominutelným faktem je, že v rámci skartačního řízení si archiv vybírá 2–3 % písemností z produkce původce. Není proto důvod nadbytečně zatěžovat veřejnoprávní původce, neboť vedení spisové služby je ve své podstatě podpůrnou činností pro výkon svěřené agendy veřejnoprávního původce.

Základní otázkou, která se bude v procesu atestací řešit, bude nákladnost této atestace. Dle názoru autorky by nesporně mělo dojít ke snížení výše úplaty za atestaci, přičemž upozorňuje na to, že nebyla odůvodněna ani její konstrukce. V původním zveřejněném znění Postupu atestačního střediska pro elektronické systémy spisové služby, při provádění atestace elektronického systému spisové služby, podmínky provádění atestace a výše úplaty za provedení atestace (VMV čá. 10/2022 (část II), s. 4) se počítalo s částkou ve výši 75 000,- Kč, která se jeví dle názoru autorky jako adekvátní. Jak již bylo výše podrobně zdůvodněno, i vedlejší, a to nemalé náklady budou pro původce nadmíru zatěžující.

6 Závěr

Cílem diplomové práce s názvem Informační systémy ve veřejné správě – elektronická spisová služba bylo analyzovat současný stav informačních systémů ve veřejné správě, a to se zaměřením na problematiku elektronické spisové služby, a zároveň navrhnout alternativní řešení odlišná od současného stavu.

Základem pro analýzu právních předpisů současného stavu elektronické spisové služby byla teoretická část práce, která se zaměřila na rešerši zákonů a odborné literatury ve státní správě, resp. u veřejnoprávních původců. Pro dobré pochopení celé problematiky spisové služby se práce v první kapitole věnovala jejímu historickému vývoji. Postupná elektronizace se nevyhnula ani spisové službě, která se transformovala ve spisovou službu elektronickou. Spisová služba se dotýká fungování každého orgánu veřejné moci a má vliv na jejich každodenní chod. Druhá a třetí kapitola práce ukazuje širší rámec elektronických systémů spisové služby ve vztahu k Evropské unii (nařízení eIDAS) a České republice v rámci eGovernmentu. Čtvrtá kapitola práce seznamuje s legislativou České republiky ve vztahu ke spisové službě a popisuje životní cyklus dokumentu. V této kapitole byla rovněž vymezena veškerá specifika spisové služby.

Ve vlastní práci byl analyzován současný stav informačních systémů ve veřejné správě se zaměřením na problematiku elektronické spisové služby jako páteřního systému. Zároveň byly analyzovány novelizace tří nejdůležitějších právních předpisů pro elektronické systémy spisové služby, kterými jsou zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů a Národní standard pro elektronické systémy spisové služby. V rámci přiblížení dané problematiky byl vybrán veřejnoprávní původce, Celní správa České republiky, na jehož příkladu byl prezentován elektronický systém správy dokumentů. Rovněž v případě tohoto subjektu bylo ukázáno řešení čtyř zvolených témat, kterými byl výstupní datový formát zpracovaných dokumentů, strojově čitelná vrstva, kontrola podpisu v rámci schvalovacího procesu a ztotožnění subjektů ve jmenném rejstříku a jejichž zhodnocení se autorka věnovala. Strojově čitelná vrstva byla vyhodnocena jako jednoznačně nadbytečná a pro výkon veřejnoprávního původce silně zatěžující. Tato témata byla posuzována rovněž z hlediska splnění požadavků v rámci chystaných atestací eSSL.

V závěru lze říci, že vytyčené cíle práce byly splněny, včetně námětů k diskusi nad otázkami nutnosti atestací elektronických systému spisové služby do budoucna.

7 Seznam použitých zdrojů

Tištěné zdroje

BROM, B. 2013. *Spisová a archivní služba ve veřejném a soukromém sektoru: praktická příručka pro správu dokumentů*. Praha: Linde Praha. 320 s. ISBN 978-80-7201-913-7.

DONÁT, J., MAISNER, M., PIFFL, R. 2017. *Nařízení eIDAS: komentář*. Praha: C. H. Beck. 300 s. ISBN 978-80-7400-633-3.

KMENT, V. 2018. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer ČR, a. s. 460 s. ISBN 978-80-7552-815-5.

KUNT, M., LECHNER T. 2017. *Spisová služba*. 2., aktualizované vydání. Praha: Leges. 384 s. ISBN 978-80-7502-233-2.

KUNT, M., LECHNER T. 2022. *Spisová služba*. 3., aktualizované vydání. Praha: Leges. 412 s. ISBN 978-80-7502-616-3.

LECHNER, T., 2013. *Elektronické dokumenty v právní praxi*. Praha: Leges. 256 s. ISBN 978-80-87576-41-0.

SKALA, L., VÍT M. 2005. *Slovníček spisové služby a archivnictví*. Ústí nad Orlicí: OFTIS. 80 s. ISBN 80-86845-31-1.

MATES, P., ČERNÝ, P., LECHNER, T., SKALKA P. 2020. *Nahlížení do spisu podle občanského soudního řádu, trestního řádu, soudního řádu správního, správního řádu a daňového řádu.* Praha: Leges, 151 s. ISBN 978-80-7502-460-2

SULITKOVÁ, L. 2017. *Archivnictví a spisová služba*. Ústí nad Labem: Filozofická fakulta, Univerzita Jana Evangelisty Purkyně v Ústí nad Labem ve spolupráci s nakladatelstvím Scientia, spol. s r.o. Acta Universitatis Purkynianae Facultatis philosophicae. 194 s. ISBN 978-80-7561-027-0.

ŠPAČEK, D. 2012. *EGovernment: cíle, trendy a přístupy k jeho hodnocení.* Praha: C. H. Beck. 258 s. ISBN 978-80-7400-261-8.

ŠTOURAČOVÁ, J. 1999. *Úvod do archivnictví*. Brno: Masarykova univerzita. 139 s. ISBN 80-210-2216-7.

ŠTĚDROŇ, B., 2007. *Úvod do eGovernmentu v České republice: právní a technický průvodce.* Praha: Úřad vlády České republiky. 171 s. ISBN 978-80-87041-25-3.

Elektronické zdroje

Česká agentura pro standardizaci. *Provozní řád 2023* [online]. [cit. 2023-10-14]. Dostupné z: https://www.agentura-cas.cz/atestace/provozni-rad/

Evropská komise. *MoReq2 specification, model requirements for the management of electronic records: update and extension, 2008* [online]. [cit. 2022-10-11]. Dostupné z: https://data.europa.eu/doi/10.2792/11981

Evropská komise. *MoReq2010, modular requirements for records systems: core services & plug-in modules (version 1.1).* Volume 1. [online]. [cit. 2022-10-11]. Dostupné z: https://data.europa.eu/doi/10.2792/2045

Evropská unie. Úřední věstník Evropské unie. *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES* [online]. [cit. 2022-10-11]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910#d1e2069-73-1

Ministerstvo vnitra České republiky. *čj. MV- 23406-1/AS-2022, Stanovisko odboru archivní správy a spisové služby k zakotvení textové vrstvy do vyhotovovaného dokumentu v digitální podobě* [online]. [cit. 2022-10-11]. Dostupné z: https://www.mvcr.cz/soubor/stanovisko-odboru-archivni-spravy-a-spisove-sluzby-k-zakotveni-textove-vrstvy-do-vyhotovovaneho-dokumentu-v-digitalni-podobe.aspx

Ministerstvo vnitra České republiky, Sbírka zákonů. *Vládní nařízení č. 29/1954 o archivnictví* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=29/1954&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, Sbírka zákonů. *Zákon č. 97/1974 Sb., o archivnictví* [online]. (PDF) [cit. 202-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=97/1974&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, Sbírka zákonů. *Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=194/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky: Sbírka zákonů. *Zákon č. 250/2017 Sb., o elektronické identifikaci* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=250/2017&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, Sbírka zákonů. *Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=259/2012&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, Sbírka zákonů. *Vyhláška č. 283/2014 Sb., kterou se mění vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=283/2014&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, Sbírka zákonů. *Zákon č. 343/1992 Sb., o archivnictví* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=343/1992&typeLaw=zakon&what=Cislo_zakona_smlouvy

Ministerstvo vnitra České republiky, *Smart Administration – Efektivní veřejná správa a přátelské veřejné služby.* [online]. (PDF) [cit. 2022-10-20]. Dostupné z: https://www.mvcr.cz/clanek/modernizace-verejne-spravy-49614.aspx?q=Y2hudW09Mw%3D%3D

Ministerstvo vnitra České republiky. Věstník Ministerstva vnitra. *VMV čá. 10/2022 (část II), Oznámení Ministerstva vnitra, kterým se zveřejňuje Postup atestačního střediska pro elektronické systémy spisové služby při provádění atestace elektronického systému spisové služby podmínky provádění atestace a výše úplaty za provedení atestace.* [online]. (PDF) [cit. 20232-10-14]. Dostupné z: https://www.mvcr.cz/soubor/vestnik-mv-castka-c-10-2022.aspx

Ministerstvo vnitra České republiky, Věstník Ministerstva vnitra. *VMV částka 27/2009* [online]. (PDF) [cit. 2023-10-11]. Dostupné z: https://www.mvcr.cz/soubor/vestnik-mv-castka-c-27-2009.aspx

Ministerstvo vnitra České republiky, Věstník Ministerstva vnitra. *VMV částka 101/2010 Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby. 2. verze* [online]. (PDF) [cit. 2023-10-11]. Dostupné z: https://www.mvcr.cz/soubor/vestnik-mv-castka-c-101-2010.aspx

Ministerstvo vnitra České republiky, Věstník Ministerstva vnitra. *VMV částka 64/2012 Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby. 3. verze* [online]. (PDF) [cit. 2023-10-11]. Dostupné z: https://www.mvcr.cz/soubor/vestnik-mv-castka-c-64-2012.aspx

Ministerstvo vnitra České republiky, Věstník Ministerstva vnitra. *VMV částka 42/2023 Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby. 4. verze* [online]. (PDF) [cit. 2023-10-11]. Dostupné z: https://www.mvcr.cz/soubor/vestnik-mv-castka-c-42-2023.aspx

Národní archiv České republiky. *Usnesení vlády České republiky ze dne 7. ledna 2004 č. 11* [online]. (PDF) [cit. 2022-10-14]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/05/chimera_usneseni.pdf

Nejvyšší správní soud. *čj. 4 Afs 264/2018-85, Sbírka rozhodnutí NSS č. 8/2022* [online]. [cit. 2022-10-11]. Dostupné z: https://sbirka.nssoud.cz/cz/rozsireny-senat-dane-datove-schranky-danove-rizeni-dorucovani-do-datove-schranky-fikce-doruceni.p4397.html?q

Vláda České republiky. Usnesením vlády č. 525 ze dne 31.května 1999. *Státní Informační politika – cesta k informační společnosti* [cit. 2023-10-11]. Dostupné z: https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/

Právní předpisy

Vyhláška 193/2009 Sb. o stanovení podrobností provádění autorizované konverze dokumentů

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

Vyhláška č. 259/2021 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky 283/2014

Vyhláška č. 85/2019 Sb., kterou se mění vyhlášky provádějící zákon o archivnictví a spisové službě

Vyhláška č. 96/2023 Sb., kterou se mění vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů

Vyhláška č. 504/2021 Sb., kterou se mění vyhlášky provádějící zákon o archivnictví a spisové službě

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů

Zákon č. 97/1974 Sb., o archivnictví

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 111/2009 Sb., o základních registrech

Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů (trestní řád)

Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších přepisů (zákon o elektronickém podpisu)

Zákon č. 255/2012 Sb., o kontrole, ve znění pozdějších předpisů (kontrolní řád)

Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, tzv. DEPO

Zákon č. 265/2017 Sb., kterým se mění zákon č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh, a zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů

Zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů

Zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o

svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Zákon č. 343/1992 Sb., kterým se mění a doplňuje zákon České národní rady č. 97/1974 Sb., o archivnictví

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů

Zákon č. 499/2004 Sb., o archivnictví a spisové službа a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

Atestace eSSL Atestace elektronických systémů spisové služby
Celní správa ČR Celní správa České republiky
ČAS Česká agentura pro standardizaci
DIA Digitální a informační agentura
DEPO Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
eIDAS Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
eIdentita Elektronická identita
eSAT Elektronický systém aplikace TranSoft
eSSL Elektronický systém spisové služby
ISVS Informační systém veřejné správy
GDPR Nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

ISDS	Informační systém datových schránek
ISVS	Informační systém veřejné správy
NA ČR	Národní archiv České republiky
NDA	Národní digitální archiv
NIA	Národní bod pro identifikaci a autentizaci
NSESSL	Národní standard pro elektronické systémy spisové služby
ZASS	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
ZOA	Zákon č. 97/1974 Sb., o archivnictví