DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Systémy správy dokumentů

Popis Systému správy dokumentů

Obecně o správě dokumentů

Od 1.7.2024 vyšla v platnost novela zákona č. 499/2004 Sb., která výrazně změnila práva a povinnosti určených původců. Důležité změny jsou obsaženy zejména v § 3a a § 69a.

Zákon č. 499/2004 Sb., o archivnictví a spisové službě popisuje především to, jak se mají původci (povinné osoby ze zákona) chovat při správě archiválií a dokumentů. Přičemž:

- **dokumentem** se myslí každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena a
- **archiválií** takový dokument, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií; archiváliemi jsou i pečetidla, razítka a jiné hmotné předměty související s archivním fondem či s archivní sbírkou, které byly vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrány a vzaty do evidence.

Platilo, že původce mohl zpracovávat dokumenty jak ve spisové službě, přičemž se stále zpřesňovalo kdy se povinnost vést spisovou službu v elektronické podobě, tak i dalších druzích informačních systémů - např. Samostatné evidenci dokumentů. V aktuálně platné verzi zákona se předpokládá vedení dokumentů pouze v elektronickém systému spisové služby (dále jen "eSSL") a systémech, které nejsou eSSL. Základní přehled rozdílů v povinnostech je uveden v následující tabulce:

Povinnost či právo	eSSL	Informační systém
Dodržovat povinnosti zákona č. 499/2004 Sb. pro eSSL	ANO	NE
Dodržovat povinnosti vyhlášky č. 259/2012 Sb.	ANO	NE
Dodržovat Národní standard pro elektronické systémy spisové služby	ANO	NE
Povinně doplňovat metadata dle vzorů DIA do dokumentů	ANO	ANO
Dodržovat spisový řád - spisový plán a skartační plán	ANO	NE
Povinnost vydávat archiválie	ANO	ANO
Právo požádat si o trvalý skartační souhlas	ANO	ANO

Obecně o spisové službě

Výkonem spisové služby se rozumí „zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností“.

Nařízení (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 (dále jen „eIDAS“) definuje pojem „elektronický dokument" jako jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvukovou, vizuální nebo audiovizuální nahrávku.

Legislativní rámec pro výkon spisové služby určuje zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (dále též „Zákon“) a prováděcí vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby. Národní standard pro eSSL (dále též „NSESSS“) vydaný Ministerstvem vnitra a publikovaný ve Věstníku Ministerstva vnitra pak stanovuje podrobné technické požadavky na aplikační a byznysové funkce eSSL. Novelizací Zákona z roku 2021 byla zavedena povinnost atestací pro eSSL (blíže v podkapitole týkající se atestací), ovšem platnost této novely byla několikrát odložena, resp. došlo k odsunu termínů, kdy tato povinnost začne platit. Aktuálně (březen 2024) je ve sněmovně před schválením další novela, která stanovuje tyto termíny:

- Od 1. ledna 2025 již nebude možné nabízet a dodávat veřejnoprávním původcům neatestované eSSL
- Od 1. ledna 2027 již bude muset většina veřejnoprávních původců využívat výlučně atestované eSSL

Z hlediska „nosiče“ můžeme pak dokumenty rozdělit na skupinu analogových (typicky dokument vyhotovený na papíru) a na skupinu elektronických dokumentů (viz nařízení eIDAS). Pojem elektronický dokument je v tomto kontextu shodný s pojmem digitální dokument.

Zákon zavádí pojem „výstupní datové formáty dokumentů“, tj. formáty, ve kterých musí původce ukládat příslušné typy digitálních dokumentů. Definice výstupních datových formátů je uvedena v § 23 vyhlášky č. 259/2012 Sb. Výstupní datové formáty jsou aktuálně definovány pro nejčastější typy digitálních dokumentů.

Zákon ě v § 3, odst. 5) stanoví podmínky pro dokumenty v digitální podobě, kde se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.

Zákon též stanoví specifické podmínky pro práci s dokumenty v digitální podobě jako je například převod mezi analogovou a digitální podobou nebo změna datového formátu.

Shrneme-li základní požadavky, pak původci musí:

1. Vykonávat spisovou službu tak, že eviduje dokumenty v eSSL.
2. Zajistit soulad eSSL s požadavky NSESSS.
3. Mít alespoň jeden eSSL.
4. Zajistit integraci mezi informačními systémy a eSSL dle požadavků NSESSS.
5. Vést jmenný rejstřík, přiřazovat subjektům bezvýznamové identifikátory a vytvářet a spravovat vazby všech dokumentů obsahujících osobní údaje na osoby ve jmenném rejstříku.
6. Řádně uchovávat a spravovat digitální dokumenty a jejich komponenty v eSSL.
7. Provádět evidenci metadat o spisech, dokumentech a dalších entitách a zajistit evidenci všech transakcí a definovaných operací v eSSL v souladu s požadavky NSESSS.
8. Zajistit příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování dokumentů ve skartačním řízení v souladu se Zákonem, vyhláškou č. 259/2012 Sb, a NSESSS
9. Zajistit řádné ověření autenticity a integrity doručených dokumentů v digitální podobě v souladu s nařízením eIDAS a zákonem č. 297/2016 Sb. a zajistit v souladu s uvedenými předpisy řádné připojení autentizačních a autorizačních prvků na dokumenty v digitální podobě vyhotovené původcem
10. Uchovávat dokumenty a umožnit výběr archiválií, vybrané archiválie v analogové podobě předávat k uložení příslušnému archivu a archiválie v digitální podobě předávat k uložení příslušnému digitálnímu archivu.

Digitální kontinuita

Digitální kontinuita je soubor procesů, opatření a prostředků nutných k tomu, aby byl původce schopen zajistit dlouhodobou důvěryhodnost informací a dokumentů. S ohledem na odlišný charakter činnosti soukromoprávních původců dokumentů a veřejnoprávních původců je u veřejnoprávních původců situace jednodušší. Pro obě skupiny původců lze však vycházet ze základních principů obsažených v ISO normách, zejména pak v ČSN ISO 30300 Systémy správy dokumentů, ČSN ISO 15489 Správa dokumentů, ČSN ISO 16363 Audit a certifikace důvěryhodných digitálních úložišť. Výše uvedené normy upravují vazby podnikových procesů

a dokumentů, zajištění vypovídací hodnoty, koncepty a principy správy dokumentů od zrodu až k uložení a zajištění dlouhodobé důvěryhodnosti.

Autenticitou dokumentů se rozumí otázka, zda jde o původní dokument: dokument je autentický, pokud nedošlo k žádné jeho změně. V případě elektronických dokumentů dokáží jejich neměnnost (označovanou též jako integritu) zajistit všechny druhy kryptografických elektronických podpisů, pečetí a časových razítek. Tedy zaručený elektronický podpis, stejně jako všechny vyšší druhy elektronických podpisů (zaručený elektronický podpis, založený na kvalifikovaném certifikátu, i kvalifikovaný elektronický podpis), zaručená elektronická pečeť, stejně jako všechny vyšší druhy elektronických pečetí, a také elektronické časové razítko.

Pravostí dokumentu se rozumí otázka, zda dokument pochází od toho, koho považujeme za jeho původce, a obecně se dovozuje z autentizačních prvků, kterými je dokument opatřen. V případě elektronických dokumentů jde o elektronické podpisy, elektronické pečeti a elektronická časová razítka. U nich se nejprve zkoumá (ověřuje) jejich platnost, která je technickým pojmem a je závislá na splnění určitých technických podmínek (podrobněji popsaných v článku 32, resp. 40 nařízení eIDAS). Teprve v případě prokázání jejich platnosti je možné, v závislosti na druhu elektronického podpisu či pečeti, z technické platnosti dovozovat i právní pravost příslušných autentizačních prvků (podpisů a pečetí), a z ní následně i pravost elektronického dokumentu jako takového.

V souvislosti s tím je nutné zdůraznit, že možnost ověřit (technickou) platnost elektronických podpisů a pečetí, stejně jako časových razítek, se s postupem času ztrácí. Jde o základní vlastnost, jakousi časovou pojistku, charakteristickou pro všechny zaručené (a vyšší) druhy elektronických podpisů, pečetí a razítek. Jejím účelem je chránit již vytvořené elektronické dokumenty před zastaráváním a oslabováním kryptografických postupů a algoritmů, použitých u jejich podpisů (ale i pečetí a časových razítek). Bez této časovém pojistky by po uplynutí určité doby již nebylo možné z technické platnosti dovozovat právní pravost podpisů, a tím ani celých dokumentů: vzhledem k oslabení kryptografických algoritmů, použitých u původně podepsaného dokumentu, by již bylo možné reálně najít (vypočítat) jiný dokument, který je tzv. kolizní vůči původně podepsanému dokumentu. Tedy takový dokument, který má jiný obsah, ale stejný elektronický podpis. Pak by bylo možné přenést elektronický podpis z původně podepsaného dokumentu na onen později vytvořený kolizní dokument, a v obou případech by byl takovýto podpis ověřen jako (technicky) platný – a nebylo by tak již možné spolehlivě prokázat, který dokument je pravý (který byl původně podepsán).

Problematika digitální kontinuity elektronických dokumentů naopak nezahrnuje otázku jejich pravdivosti neboli správnosti obsahu těchto elektronických dokumentů. Požadavek na dlouhodobě zajištění, resp. dlouhodobé udržování digitální kontinuity elektronických dokumentů se v praxi týká jen těch elektronických dokumentů, u kterých je nějaký důvod pro zachování možnosti prokázat jejich autenticitu a pravost.

Výběr a dlouhodobá archivace digitálních dat

Výběr a dlouhodobá archivace digitálních dat (dokumentů) probíhá dle zákona o archivnictví č. 499/2004 Sb., kde je dokument definován v § 2 písm. e) jako „každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, která byla původcem vytvořena nebo byla původci doručena“.

Povinnost uchovávat dokumenty a umožnit výběr archiválií má naprostá většina právnických osob působících v ČR. Tyto subjekty označuje Zákon jako původce dokumentů (viz § 3 Zákona). Novela Zákona platná k 1.7.2024 zavádí navíc § 3a, dle kterého veřejnoprávní původci musí evidovat dokumenty a umožnit jejich výběr (export dle standardu stanoveným Národním archivem) nejen ze systémů eSSL, ale i z dalších informačních systémů, které využívají. De facto se tedy jedná o zavedení standardu Archiving by Design.

Archivně relevantní informace se vyskytují také řadě dalších prostředí, ať jsou to **databáze, specializované IS** (např. GIS, CAD, BIM), **webové stránky či sociální sítě, ze kterých se také provádí výběr a jsou trvale ukládány v prostředí digitálního archivu**.

Problematiku výběru dokumentů (informací) trvalé hodnoty, tedy archiválií, a jejich exportu do digitálního archivu řeší také vyhláška č. 360/2023 Sb., o dlouhodobém řízení ISVS. Již při vzniku systémů je třeba pamatovat na možnost exportu dat z nich a to jak pro účely migrace dat do jiného systému nebo pro archivní

účely. Archiváři by měli mít možnost již při vzniku systému definovat archivně cenné informace, podobu jejich výstupu a proces přenosu do digitálního archivu (***Archiving by Design***).

Řídící dokumenty

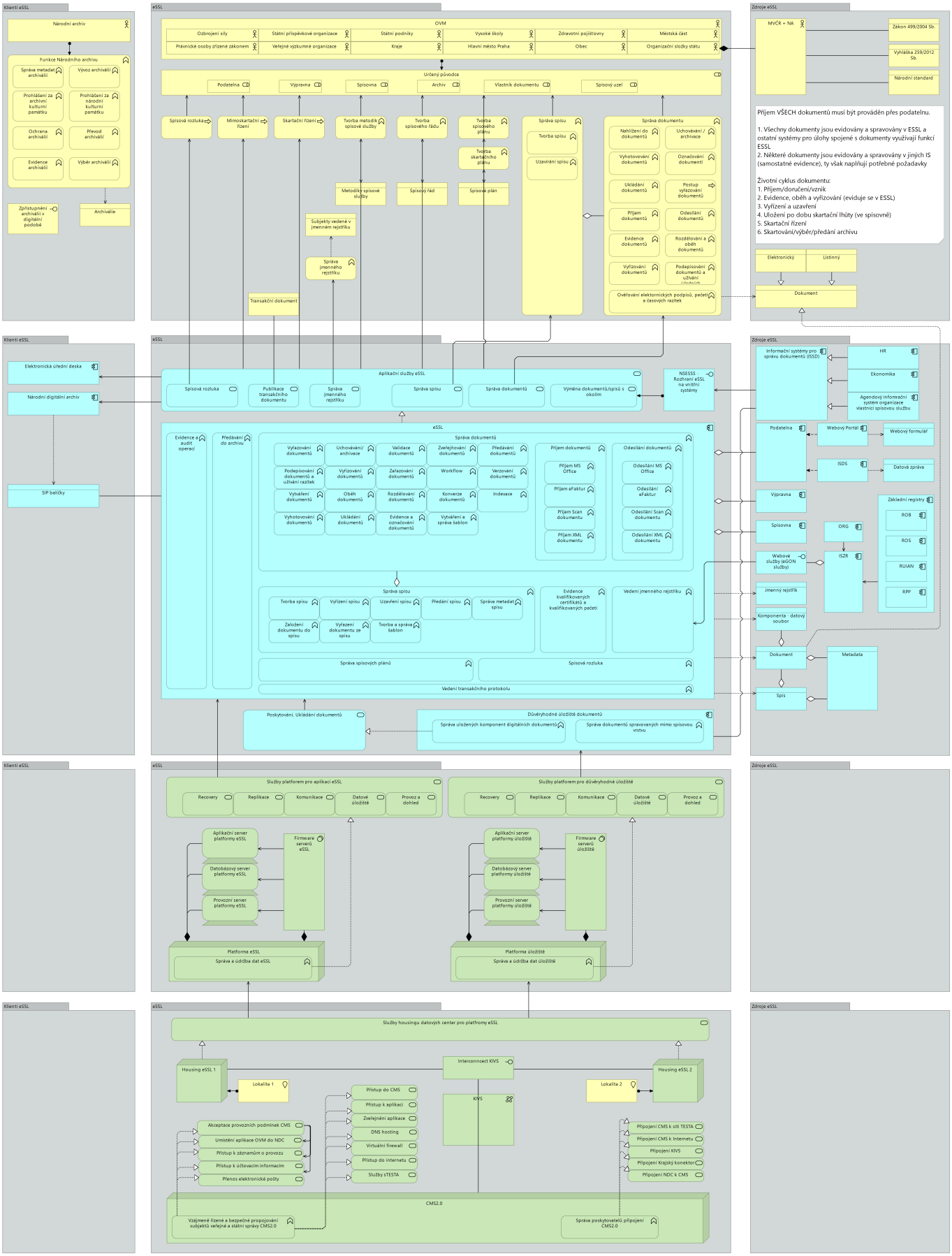
V rámci výkonu spisové služby jsou řídícími dokumenty zejména:

- Legislativa
    1. Zákon č. 499/2004 Sb., o archivnictví a spisové službě
    2. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
    3. Národní standard pro elektronické systémy spisové služby
- Technické a architektonické požadavky
    1. Národní architektonický plán
- Vnitřní řídící dokumenty úřadu
    1. Spisový řád (jehož součástí je spisový a skartační plán a podpisový řád)
    2. Informační koncepce úřadu
- Dokumentace k elektronickému systému spisové služby
    1. Provozní dokumentace k eSSL dle vyhlášky č. 360/2023 Sb., o dlouhodobém řízení ISVS
    2. Dokumentace k integracím eSSL a jiných informačních systémů
    3. Dokumentace související s výkonem spisové služby

Další zdroje

V souvislosti s výkonem spisové služby existuje celá řada dalších zdrojů informací a metodických dokumentů publikovaných zejména Odborem archivnictví a spisové služby (OAS) Ministerstva vnitra a Národním archivem (např. INFORMAČNÍ LIST pro otázky elektronické spisové služby a dokumentů v digitální podobě).

Pohled na systém správy dokumentů



Pravidla pro systémy správy dokumentů

Spisovou službu považujeme za společnou schopnost na úrovni úřadu (capability), kde většina principů je

shodných napříč celým úřadem (motivační vrstva, aplikační vrstva eSSL a integrace, byznysová vrstva procesů a funkcí a interakcí) a na úrovni jednotlivých agend se odlišuje dle výkonu dané agendy minimálně. Architekturu výkonu spisové služby tedy je třeba zahrnout do mapy schopností úřadu.

Při zpracování Enterprise architektury úřadu i při zpracování a realizaci jednotlivých architektur, týkajících se ať už agend nebo schopností, nebo jejich řešení, je nutno zahrnout spisovou službu jako obecnou schopnost a správným způsobem řešit její realizaci. Je přitom nutno zvážit, do jaké míry je faktický i technický výkon spisové služby společný v rámci celé organizace a jestli a jakým způsobem se bude lišit v rámci jednotlivých agend či řešení. Jednoznačným doporučením je mít jeden eSSL a u ostatních informačních systémů zajistit úkony spojené se správou dokumentů (příloh k transakcím) a s výkonem spisové služby formou integrace na eSSL rozhraním.

Součástí architektury úřadu by tedy z pohledu spisové služby měly být vždy alespoň následující elementy:

- Elektronický systém spisové služby (splňující požadavky NSESSS) včetně modulů podatelny a výpravny umožňující příjem a odesílání i digitálních dokumentů správnými komunikačními kanály
- Jmenný rejstřík (může být i samostatnou komponentou), nejlépe integrovaný na rejstřík kmenových dat klientů úřadu, notifikovaný ze základních registrů.
- Spisovna pro uchování uzavřených spisů a vyřízených digitálních dokumentů po dobu skartační lhůty (eSSL je spisovnou pro dokumenty v digitální podobě)
- Rozhraní eSSL zajišťující úkony spojené s dokumenty a procesy evidence dokumentů a správy jejich metadat v eSSL formou aplikačních služeb pro další informační systémy úřadu (systémy, které dokumenty nespravují)

Hovoříme-li o integraci informačních systémů s eSSL a o správě úkonů spojených s dokumentem, může tato integrace být na úrovni byznysových objektů a jejich metadat řešena v souladu s následujícími pravidly:

1. Digitální dokument, respektive jeho komponenty a datové soubory, jsou uloženy v úložišti digitálních dokumentů, které zajišťuje péči o digitální soubory
2. Metadata o dokumentu jsou spravována:
    - eSSL, nebo
    - informačním systémem
3. Se soubory v úložišti jsou oprávněny pracovat:
    - eSSL, nebo
    - informační systém
4. Ve Jmenném rejstříku se vede evidence údajů o subjektech, jejichž se týkají dokumenty evidované ve spisové službě

Atestace eSSL

Novelou Zákona z roku 2021 (§ 69b-d) bylo stanoveno, že veřejnoprávní původci budou postupně muset přejít a využívat výhradně systémy eSSL, které jsou atestované. Atestace budou prováděny atestačním střediskem, které určí Ministerstvo vnitra (v současnosti je určena agentura ČAS), případně pokud není určeno, tak samotným ministerstvem. Proces atestace není pouze formální, ale spočívá v tom, že atestační středisko provede funkční testy dle stanovených atestačních scénářů . Atestační scénáře jsou veřejně dostupné na stránkách agentury ČAS . V případě, že eSSL splňuje podmínky stanovené Zákonem, vyhláškou a NSESSS, tak středisko vydá vystaví žadateli písemný atest (platný 2 roky), který je následně zveřejněn, jak na stránkách střediska, tak i ve Věstníku MV. Novelizace z roku 2024 přináší několik zásadních změn:

- Posun lhůt
    - Od 1. ledna 2025 zákaz nabídky a dodávky neatestovaných eSSL veřejnoprávním původcům
    - Od 1. ledna 2027 bude muset většina veřejnoprávních původců již využívat výhradně atestovaný eSSL
- Vyjmutí malých obcí a škol z povinnosti mít atestovaný eSSL
- Vyjmutí a úprava povinností IS bezpečnostních složek v oblasti atestace eSSL
- Veřejnoprávní původci, resp. jejich IS (nejenom eSSL), budou muset umět dokumenty opatřovat strojově čitelnými metadaty

- Reatestace zůstává 1x za 2 roky a pokud se v tomto období změní legislativa či technické podmínky (např. uvolnění nového releasu, ovšem bez zásadních změn), tak je možné daný eSSL využívat až do konce platnosti původního atestu a reatestovat ho až v další dvouroční lhůtě
    - MV může v případě pochybností (např. na základě kontroly) zažádat středisko o reatest

Vazby na architekturu informačního systému veřejné správy

V rámci architektury každého informačního systému veřejné správy sloužícího pro podporu výkonu činností agendy veřejné správy je nutno myslet také na oblast výkonu spisové služby. Vzhledem k tomu, že prakticky v každé agendě veřejné správy se buď vytváří, nebo zpracovávají, nebo odesílají, nebo evidují dokumenty, anebo u ní dochází k zápisu záznamu do spisu (z pohledu legislativy týkající se spisové služby), je nutno zajistit úkony spojené se spisem a dokumentem. Splnění povinností je tedy možné pouze pomocí eSSL splňující požadavky NSESSS.

Vazby na architekturu provozních systémů

Velice často se zapomíná na to, že výkon spisové služby se týká všech dokumentů, a tedy nejen úředních dokumentů typu podání a rozhodnutí v rámci výkonu agend veřejné správy. U veřejnoprávních původců se jedná o evidenci a správu veškerých dokumentů (s výjimkou těch, které si daný původce odůvodněně vyňal z evidence ve svém spisovém řádu), a tedy je nutno zajistit výkon spisové služby v elektronické podobě také pro pracovní a provozní dokumenty. To se týká jak dokumentů pracovního charakteru (zápisy z porad, organizační a řídící dokumenty, řídící akty, interní sdělení), tak ale také všech dokumentů ekonomického a provozního charakteru (faktury, objednávky, smlouvy ekonomické doklady, personální dokumentace, žádanky, závěrky a výkazy apod.).

V případě provozních informačních systémů jednoznačně doporučujeme jejich integraci na eSSL. Zejména u ekonomických informačních systémů, systému pro řízení personalistiky a mezd a zdrojů a dalších manažerských informačních systémů týkajících se různých žádanek, evidencí, a workflow procesů, se dost často na výkon spisové služby zapomíná. Zde je vhodná integrace na eSSL, neboť zajištění splnění všech požadavků NSESSS pro tyto systémy by s sebou přineslo neúměrné finanční náklady spojené s pořízením a rozvojem těchto provozních IS. Integrací na eSSL se také zajistí řádné realizování skartačních řízení u těchto druhů dokumentů.

Souvislosti s architekturou údajů o subjektech

Určení původci, kteří vykonávají spisovou službu v elektronické podobě, musejí podle § 64, odst. 4 až 8, Zákona č. 499/2004 Sb., o archivnictví a spisové službě provozovat jako samostatnou komponentu takzvaný "Jmenný rejstřík", kam zapisují určené minimální údaje o všech subjektech, kterých se týkají jimi evidované dokumenty.

Realizace propojení jmenného rejstříku a ostatních komponent, respektive realizace procesů evidence subjektů je následující:

- V úřadu je u každého eSSL jako logická komponenta i Jmenný rejstřík. Funkce Jmenného rejstříku může za splnění všech dalších podmínek zastávat i zdroj evidence subjektů.
- Do jmenného rejstříku se evidují údaje o všech subjektech, kterých se týkají evidované dokumenty a to s využitím AIFO fyzických osob v agendě spisové služby, nikoliv v agendách, ve kterých se o osobách úřaduje. Pro vazby jmenného rejstříku na eSSL a další evidence dokumentů je třeba využívat interní identifikátor, nikoliv AIFO.
- Evidence subjektů ve Jmenném rejstříku a evidence subjektů za účelem úřadování v agendě jsou dvě oddělené věci, proto je nutno dbát na správné postupy, viz související kapitoly k evidenci subjektů a identifikátorům.

Výběr a dlouhodobá archivace digitálních dat

Výběr archiválií z dokumentů provádí příslušný archiv podle své působnosti a to nejpozději po uplynutí uschovacích (skartačních) lhůt s tím, že ideální je označit podstatná data za archiválie mnohem dříve. Kritériem výběru je trvalá hodnota dokumentu daná mj. jeho hospodářským, právním, politickým, informačním, historickým, kulturním nebo vědeckým významem. Veškeré archiválie jsou **evidovány** jako součást národního archivního dědictví. Úkolem archivů je dále trvalé **uložení** archiválií a jejich **ochrana**, archivní **zpracování a zpřístupnění**.

Digitální archiválie lze uchovávat pouze v akreditovaném digitálním archivu metodika. Od roku 2015 je zatím jedinou infrastrukturou tohoto typu **Národní digitální archiv (NDA)** provozovaný Národním archivem. Ten na Národním archivním portále (NArP) mj. nabízí nástroje pro skartační řízení a přejímku digitálních archiválií.

Výstupní formáty dle pravidel stanovených vyhláškou č. 259/2012 Sb. pokrývají nejběžnější typy dokumentů . U původců se však mohou vyskytovat i jiné typy dokumentů, u kterých není výstupní formát vyhláškou určen. Mimo jiné i proto, že na jeho stanovení není všeobecná shoda. Z hlediska dlouhodobé archivace i potřeb veřejné správy by však bylo přínosné, kdyby existoval registr formátů shrnující vhodnost používání určitého formátu. Proto také vznikl Národní standard formátů pro archivaci, který určuje, jaký formát je pro různé typy dokumentů (dokument tak, jak jej definuje zákon o archivnictví) vhodný k archivaci.

Důležitým zdrojem pro výběr archiválií jsou dokumenty spravované v eSSL. Archivy provádějí dohled nad vedením eSSL a následně dokumenty vybírají ve skartačním řízení k trvalému uložení. Dalšími zdroji dokumentů pro výběr archiválií jsou informační systémy, které spravují dokumenty.

Možné způsoby zajištění digitální kontinuity dokumentů

Je velmi důležité pamatovat na problematiku digitální kontinuity a o své elektronické dokumenty se aktivně starat. Veřejnoprávní původci musí zajistit evidenci dokumentů v systému spisové služby. Oba výše uvedené způsoby pak musí splňovat požadavky Národního standardu pro elektronické systémy spisové služby v souladu se zákonem č. 499/2004 Sb. Zaměříme-li se na elektronické dokumenty ve smyslu nařízení eIDAS, pak budeme hovořit o elektronickém systému spisové služby a elektronických evidencích dokumentů. Jedním z klíčových požadavků Národního standardu je existence tzv. transakčního protokolu – zápisu provedených operací uskutečněných v rámci elektronického systému spisové služby v elektronické podobě. Transakční protokol v případě elektronických dokumentů zajišťuje, že od okamžiku zaevidování dokumentu až do okamžiku jeho předání do archivu nebo okamžiku vyřazení a zničení je systematicky evidována jakákoliv operace týkající se evidovaného dokumentu. Tímto je zcela jednoznačně po dobu životního cyklu dokumentu zajištěno, že lze v rámci evidenčního systému garantovat určité vlastnosti elektronického dokumentu, zejména pak věrohodnost původu a neporušenost obsahu. U každého elektronického dokumentu musí být rovněž zajištěna po celou dobu životního cyklu jeho čitelnost, a to jak v technickém slova smyslu, tak z pohledu jeho uživatelsky vnímatelné podoby.

U veřejnoprávních původců je s ohledem na výše zmíněný požadavek prokázání věrohodnosti původu a neporušitelnosti obsahu dokumentu stanovena zákonná povinnost ověřování elektronických podpisů, elektronických pečetí a elektronických časových razítek, pokud je příchozí elektronický dokument obsahuje. Uvedení původci jsou ze zákona povinni výsledky ověření zaznamenat ve svých evidenčních systémech, které jak bylo uvedeno výše, musí splňovat zákonem stanovené požadavky, včetně požadavku na vedení transakčního protokolu. Proto není nutné po prvotním ověření u veřejnoprávních původců používat takové metody, jaké se používají běžně pro zajištění „věrohodnosti původu“ u soukromoprávních původců - například není nutné opětovně opatřovat elektronické dokumenty časovými razítky před jejich expirací a podobně - věrohodnost původu elektronických dokumentů je u veřejnoprávních původců zajištěna řádnou systematickou evidencí dokumentů v určených systémech, kde je navíc pomocí transakčního protokolu možné po celou dobu životního cyklu dokumentu prokázat veškeré operace, které se s evidovaným dokumentem uskutečnily - tj. pro prokázání věrohodnosti původu je zcela dostačující systematická evidence a transakční protokol[1)].

Výše uvedené lze u veřejnoprávních původců i snadno ověřit – audit systémů zajišťujících vedení spisové služby je možné realizovat v průběhu času a každý veřejnoprávní původce má zákonem stanovenou povinnost kontroly těchto činností. Elektronické systémy spisové služby splňují z pohledu zákona o kybernetické bezpečnosti charakteristiku tzv. významného informačního systému, neboť v případě jejich výpadku nebo nesprávného fungování by veřejnoprávní původci nemohli plnit řádně a souvisle svůj výkon. S ohledem na to by tyto měly být jako významné informační systémy identifikovány a oznámeny Národnímu úřadu pro kybernetickou a informační společnost procedurou dle kybernetického zákona. Tím se tyto systémy dostanou rovněž pod pravidelný dohled útvarů zajišťujících kybernetickou bezpečnost.

Elektronické systémy spisové služby zpracovávají osobní údaje fyzických osob, proto veřejnoprávní původci nad těmito systémy mají s ohledem na povinnosti vyplývající z obecného nařízení na ochranu osobních údajů a ze zákona o zpracování osobních údajů řadu povinností, které též zvyšují celkovou důvěryhodnost systémů, ve kterých veřejnoprávní původci evidují své dokumenty.

Výše uvedenými opatřeními lze u veřejnoprávních původců zcela spolehlivě prokázat věrohodnost původu a to i u přijatých dokumentů obsahující elektronické podpisy, elektronické pečetě a elektronická časová razítka a to bez nutnosti jejich opětovného opatřování časovými razítky nebo jinými autentizačními či autorizačními prvky.

Možné problémy

Možným rizikem zajištění digitální kontinuity založeného na základě transakčních protokolů eSSL je problematika kolizních dokumentů. Jedná se o situaci, kdy je do transakčního protokolu v souladu s NSESSS poznamenán otisk (tzv. hash) dokumentu spolu s označení použitého hashovacího algoritmu, ovšem stejný hash může odpovídat i jiným dokumentům. Následně není možné, především u přijatých dokumentů, dovodit o jakém dokumentu (skrze jeho hash) transakční protokol pojednává, což výrazně komplikuje případné dosvědčení právní validity.

Pro eliminaci tohoto rizika, lze využít postupy, kterými se prodlužuje ověřitelnost podle standardu ETSI (The European Telecommunications Standards Institute) a který odpovídá předpisům eIDAS. Jde tedy o opakovaného přidávání kvalifikovaných elektronických časových razítek a validačních informací sloužící k prodlužování možnosti ověření platnosti podpisů a pečetí na elektronických dokumentech. Zjednodušeně lze říci, že tato opatření mají charakter nového elektronického podepsání, nového zapečetění či nového opatření kvalifikovaným elektronickým časovým razítkem. Tyto možnosti totiž znamenají, že se na autentizaci původního dokumentu použijí aktuálně dostatečně silné kryptografické postupy a algoritmy (konkrétně dostatečně robustní hashovací funkce a dostatečně velké klíče), a tím je – opět na určitou dobu – dostatečně ztíženo hledání kolizních dokumentů. Vzhledem k různým právním účinkům elektronických podpisů (představujících projev vůle), elektronických pečetí (představujících vyjádření původu) a časových razítek (představujících „fixaci v čase“) se v praxi, k prodloužení možnosti ověření platnosti původních podpisů a pečetí, využívají právě kvalifikovaná elektronická časová razítka. Důležité je, aby každý jednotlivý krok tohoto dlouhodobého procesu byl proveden včas. Tedy aby další časové razítko bylo přidáno ještě dříve, než zaúčinkuje tzv. časová pojistka (než skončí v čase omezená možnost ověření původního podpisu či pečeti). Případně promeškání nejzazšího okamžiku způsobí, že pozdě přidané časové razítko již nemá prodlužující účinek.

V praxi přitom není nutné (včas) přidávat časová razítka k jednotlivým dokumentům. Vhodnými postupy je možné minimalizovat spotřebu časových razítek, například společným umístěním více dokumentů (či pouze jejich otisků) do vhodného kontejneru (ASiC), a časovými razítky opatřovat pouze kontejner jako takový. Sdružování do kontejnerů je vhodné dle logického spojení dokumentů, například do úrovně spisů. Stejně tak není podstatné, kdo podniká výše naznačená opatření, nutná pro zajištění digitální kontinuity dokumentů.

Je však nutné konstatovat, že ač riziko kolizních dokumentů existuje, současné legislativní prostředí nedává veřejnoprávním původcům dostatečný prostor k rozhodnutí a vlastnímu zvážení rizik a dodatečné připojování elektronických pečetí či časových razítek by mohlo být v rozporu s péčí řádného hospodáře, neboť u nákladů na zajištění takového postupu by se mohlo jednat o neúčelně vynaložené prostředky veřejného rozpočtu.

Dalším možným řešení je předávání transakčních protokolů do archivu v krátké lhůtě.

eSSL, Spisová služba, Funkční celek, spisovka

[1)]

Může být v rozporu eIDAS ver 2.0, recitál 33 a 33a a článek 45 g a článek 45ga (jde o draft)
https:%%//%%data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/cs/pdf