DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

<title>Pravidla pro Systémy správy dokumentů</title>

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 elektronický systém spisové služby a u ostatních informačních systémů, včetně agendových informačních systémů a provozních informačních systémů, zajistit úkony spojené se správou dokumentů (příloh k transakcím) a s výkonem spisové služby formou integrace na elektronický systém spisové služby předepsaným rozhraním.

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

- Elektronický systém spisové služby (splňující požadavky Národního standardu) 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
- 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 (agendové, provozní)
- Informační systémy spravující dokumenty integrované na rozhraní ESSL

Jelikož legislativa obecně počítá s tím, že v rámci úřadu je vždy provozován jeden ESSL a ostatní agendové a provozní informační systémy jsou na něj integrovány a úkony spojené s dokumenty se realizují formou rozhraní ESSL, měla by v úřadu být implementována integrace všech informačních systémů spravujících dokumenty (pokud nejsou samy samostatnou evidencí dokumentů v elektronické podobě) s ESSL a samotný ESSL navázán na úložiště pro uchovávání komponent digitálních dokumentů. Na obrázku níže je znázorněn obecný stav pochopení integrace elektronického systému spisové služby za využití jednoho centrálního úložiště pro digitální dokumenty.

Hovoříme-li o integraci informačního systému s elektronickým systémem spisové služby 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 evidenčním nástrojem, tedy:
    - Elektronickým systémem spisové služby, nebo
    - informačním systémem, který plní funkci samostatné evidence
3. Se soubory v úložišti jsou oprávněny pracovat:
    - elektronický systém spisové služby, nebo
    - informační systém sloužící jako samostatná evidence, nebo
    - informační systém integrovaný na ESSL prostřednictvím ESSL
4. Ve Jmenném rejstříku se vede evidence údajů o subjektech, jejichž se týkají dokumenty evidované ve spisové službě

Vazby na architekturu agendového informačního systému

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. Vesměs existují dvě formy, jak zajistit povinnosti výkonu spisové služby v souvislosti s daným AISem, a to následující:

1. Integrovat AIS na ESSL prostřednictvím předepsaného rozhraní a zajistit, aby úkony spojené s dokumentem vykonával AIS prostřednictvím tohoto rozhraní.
2. Zajistit, aby daný AIS splňoval požadavky Národního standardu pro ESSL kladené na tzv. „samostatnou evidenci“ a vykonávat úkony spojené s dokumenty a všechny procesy týkající se výkonu spisové služby v samostatné evidenci tímto systémem.

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 a neúřední 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 elektronický systém spisové služby. 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 Národního standardu na samostatné evidence 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 jež 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.

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 a to buď v systému spisové služby, nebo v samostatných evidencích dokumentů. 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 nebo v rámci samostatné evidence dokumentů 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.

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, ale i některé významné samostatné evidence dokumentů (typicky agendové informační systémy), 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 a samostatné evidence dokumentů též 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.